Fast-Decodable Asymmetric Space-Time Codes from Division Algebras

Roope Vehkalahti, *Member, IEEE*, Camilla Hollanti, *Member, IEEE*, and Frédérique Oggier

***Abstract*—Multiple-input double-output (MIDO) codes are important in the near-future wireless communications, where the portable end-user device is physically small and will typically contain at most two receive antennas. Especially tempting is the 4×2 channel due to its immediate applicability in the digital video broadcasting (DVB). Such channels optimally employ rate-two space-time (ST) codes consisting of (4×4) matrices. Unfortunately, such codes are in general very complex to decode, hence setting forth a call for constructions with reduced complexity.**

Recently, some reduced complexity constructions have been proposed, but they have mainly been based on different *ad hoc* methods and have resulted in isolated examples rather than in a more general class of codes. In this paper, it will be shown that a family of division algebra based MIDO codes will always result in at least 37.5% worst-case complexity reduction, while maintaining full diversity and, for the first time, the non-vanishing determinant (NVD) property. The reduction follows from the fact that, similarly to the Alamouti code, the codes will be subsets of matrix rings of the Hamiltonian quaternions, hence allowing simplified decoding. At the moment, such reductions are among the best known for rate-two MIDO codes [4], [5]. Several explicit constructions are presented and shown to have excellent performance through computer simulations.

***Index Terms*—Coding gain, cyclic division algebra, digital video broadcasting next generation handheld (DVB-NGH), fast maximum-likelihood (ML) sphere decoding, Hamiltonian quaternions, Hasse invariants, lattices, low-complexity space-time block codes (STBCs), multiple-input single/double/multiple-output (MISO/MIDO/MIMO), non-vanishing determinant (NVD), orders.**

I. Introduction

Among known space-time codes, the Alamouti code [6] and the fully diverse 4×1 quasi-orthogonal codes [7] stand out due to their orthogonality properties that are beneficial for decoding. Both of these codes however have a low code rate, hence best suitable for an asymmetric transmission, where there are less receive antennas than transmit antennas. It is far from obvious how to generalize these codes to asymmetric scenarios where we demand higher code rates and different number of antennas. On the other hand, the now well known cyclic division algebra (CDA) codes designed for a symmetric transmission have full rate and are generalizable to an arbitrary number of antennas. Unfortunately, they are very complex to decode, especially when we have less receive antennas than transmit antennas. Yet there is a strong demand for asymmetric codes that would be fast-decodable, generalizable to more antennas, and would support higher rates. The special case of two receive antennas is referred to as a multiple input-double output (MIDO) code.

For example one of the most interesting wireless applications currently is the design of 4×2 MIDO codes. Such asymmetric systems can be used in the communication between, for instance, a TV broadcasting station and a portable digital TV device. The four transmitters can either be all at one station or separated between two different stations in this way providing better coverage in the case when the transmission of one of the stations is blocked out by a deep shadow.

In Europe, the digital video broadcasting (DVB) consortium has adopted different standards for terrestrial (DVB-T) fixed reception, handheld (DVB-H) reception, satellite (DVB-S) reception as well as an hybrid reception like DVB-SH. The ongoing work towards the standardization of the DVB Next Generation Handheld (NHG, see the DVB Project's web page [8] for more information) systems is bringing this topic ever more to the forefront of current MIMO research. The inclusion of the 4×2 systems in the consortium's call for technologies for the DVB-NGH indicates having a MIDO code in the coming standard.

One solution to the 4×2 code construction problem could be to use a full-rate CDA code, *e.g.* the 4×4 Perfect code [9]. However, when received with two antennas, a rate-four code cannot be optimally decoded with a linear decoder such as a sphere decoder. Codes especially designed for the 4×2 channel have been proposed in *e.g.* [10], [11], [12], but all the codes require high complexity maximum-likelihood (ML) decoding, namely full-dimensional sphere decoding.

A natural approach to this design problem is to imitate

Part of this work appeared at ISIT 2010 [1], at SPCOM 2010 [2], and at ISITA 2010 [3].

the form of the code matrices of the already known fast-decodable codes or use these codes as building blocks for higher rate codes. The key problem in such constructions is that it is very hard to guarantee that the resulting code will still have good performance, thus in many cases requiring optimization to be carried out through extensive computer searches.

In this paper we are going to adopt a different approach to this problem. We study the algebraic structure of known fast-decodable codes like the Alamouti code and the division algebra based quasi-orthogonal codes. By analyzing the relation between the Hasse-invariants and the geometric structure of these codes we are able to distill the key algebraic properties that force these codes to be fast-decodable. This approach then depicts an infinite family of fast-decodable codes from division algebras.

The main advantage of our take on this subject is that the proposed codes are based on orders of division algebras and therefore they are not only fast-decodable, but are also guaranteed to have full-diversity, the non-vanishing determinant (NVD) property, and further allow us to perform algebraic minimum determinant optimization. We can show, under given conditions, that the ML decoding complexity of a MIDO code will always be reduced by at least 37.5%, while maintaining the NVD. Explicit constructions based on the proposed criteria will be provided. One of the examples introduces a code that has comparable performance with the best known fast-decodable ST codes [4], [5] and further has (provable) NVD. The proposed theory provides fully diverse, fast-decodable (FD) codes with the NVD property for any even number n_t of Tx antennas and any code rate $\leq n_t/2$. Motivated by the DVB-NGH, most of the examples are given in the case of 4 Tx antennas and 2 Rx antennas.

We make the typical assumption of transmission over a coherent i.i.d. Rayleigh fading channel with perfect channel state information at the receiver (CSIR) and with no CSIT,

$$Y = HX + N,$$

where Y, X, H, N are the received, transmitted, channel, and the Gaussian noise matrix, respectively. The ST matrix $X \in M_{n_t}(\mathbb{C})$, while $Y, H, N \in M_{n_r \times n_t}(\mathbb{C})$, where n_t (resp. n_r) denotes the number of transmit (resp. receive) antennas. We assume no correlation, but in the correlated case the transmitter can adapt to the rate-one code naturally embedded within the proposed codes while maintaining and even improving fast decodability.

A. Related work

The first reduced ML-complexity 4×2 construction was given in [4], combining two copies of a quasi-orthogonal code [13]. This resulted in a MIDO code that does have lower decoding complexity, but unfortunately does not have full rank. Nevertheless, good performance is still achieved at low-to-moderate SNRs and with four real dimensions less in the sphere decoder.

The most recent results on fast-decodable codes have appeared in [5], where new constructions with optimized performance have been presented, and in [1], [2], [3], where fast-decodable codes with the NVD property have been built from crossed product and cyclic presentations of division algebras. In the preprint [14] the authors consider quadratic forms as a tool for characterizing the decoding complexity, and in the preprint [15] multi-group ML-decodable collocated and distributed space-time codes are proposed.

B. Organization and contributions

The rest of the paper is organized as follows. We start by giving some background on space-time codes with a lattice structure and their decoding via sphere decoding in Section II. The concept of fast decodability is then defined and illustrated in Section III, where the role of the Alamouti code is emphasized. To pursue the study of fast-decodable codes, we then focus on CDA codes in Section IV, where some background and further motivating examples are presented, translating fast decodability into being able to embed the considered cyclic algebra into an algebra of matrices with quaternionic coefficients. The conditions guaranteeing the existence of such an embedding are studied in Section V: we need an algebra whose center is totally real and such that all its infinite places ramify in the algebra. A family of such cyclic algebras is provided. A last design criterion, the normalized minimum determinant, is added and bounds on optimal lattice codes with respect to it are computed in Section VI. Different explicit construction methods are described in Section VII. Finally, several code constructions are presented in Section VIII for 4×2 codes followed by simulation results in Section IX. In Section X the results are extended for more transmit antennas and explicit constructions are provided for 6×3 and 6×2 codes.

Further generalizations are provided in Section XI, where it is also shown that the existence result can be made explicit via conjugations of the familiar left-regular representation. Section XII concludes the paper. In Appendix, relevant algebraic results related to central simple algebras and Hasse invariants are presented.

The main contributions of this paper are listed below.

- General methods to produce space-time lattice codes with the NVD property and given geometric structure are given.
- A unified construction of families of CDAs that can be embedded into matrix rings of the Hamiltonian quaternions $M_k(\mathbf{H})$ is provided. The underlying algebraic principles are studied in full detail. It is then demonstrated how such a structure can be beneficial in the decoding. The generality of the constructions is in contrast to the present *ad hoc* constructions available in the literature.
- A complete solution to the discriminant minimization problem [16] for division algebras with arbitrary centers is given. As an application a normalized minimum determinant bound for code lattices in $M_k(\mathbf{H})$ is derived from the algebraic results.
- We mainly consider the 4×2 MIDO case, but also provide constructions for the 6×2 and 6×3 cases. The methods are generalizable to any even number of Tx antennas.
- The main difference with other fast-decodable MIDO codes is that all the proposed codes have the NVD property. The proofs for the NVD are based on the underlying algebraic structure of the code and hold for infinite constellations. This can be seen as an improvement for [5], where the NVD is conjectured by computing the minimum determinant for certain finite QAM alphabets.
- We build explicit codes that have 25-37.5% reduced decoding complexity for general constellations, and whose performance is comparable to the best known MIDO codes. Such complexity is among the best known for the MIDO channel, and can be further reduced by using a symmetric alphabet – a square QAM alphabet, for instance. No fast-decodable MIDO codes with provable NVD other than the ones in this paper have been reported.

C. Notations

Throughout the paper, we will use the following notations:

- Tx for transmit antennas, Rx for receive antennas,
- $n_t \times n_r$ for a channel with n_t Tx and n_r Rx antennas,
- $(n \times k)$ for matrix dimensions,
- boldface lowercase letters for vectors, *e.g.* $\mathbf{g} = (g_1, \ldots, g_t)$ or $\mathbf{g} = (g_1, \ldots, g_t)^T$,
- capital letters for matrices, *e.g.* X or M,
- x^* for the complex conjugate of x, X^* for element-wise conjugation in a matrix X, and $X^\dagger$ for the Hermitian conjugate of X,
- calligraphic letters for algebras, *e.g.* $\mathcal{A}$,
- E/K for number field extensions and σ for the generator of a cyclic Galois group $\mathrm{Gal}(E/K)$. Note that K is also used for the rank of a lattice in some instances, but this should cause no danger of confusion.
- The field norm from E to K is denoted by
$$\mathcal{N}_{E/K}(x) = x\sigma(x)\cdots\sigma^{n-1}(x) \in K,$$
where $n = \#\,\mathrm{Gal}(E/K)$.

II. Space-time lattice codes

We start with as general a definition of a space-time code as possible, and motivate why we focus our attention to *space-time lattice* codes, which furthermore can be decoded via sphere decoder, a universal decoder for lattice codes. We explain in detail how this is done.

A. Definitions

Abstractly, a space-time codeword X is an $(n \times k)$ matrix with coefficients in $\mathbb{C}$, where n corresponds to the number of transmit antennas, and k is the coherence time (or delay) during which the channel is assumed constant. We will, in this paper, concentrate on the case $k = n$, so that a space-time code is a square matrix, corresponding to minimum delay codes.

Definition 2.1: A *space-time code* $\mathcal{C}$ is a set of $(n\times n)$ complex matrices. We often use the abbreviation *STBC* for *space-time block code*.

The space $M_n(\mathbb{C})$ of $(n \times n)$ matrices with complex coefficients is a vector space of dimension

$$\dim_{\mathbb{R}}(M_n(\mathbb{C})) = 2n^2$$

over the reals. Therefore, for every code $\mathcal{C} \subseteq M_n(\mathbb{C})$, we can consider, following [15], the subspace $\langle\mathcal{C}\rangle$ spanned by the matrices of $\mathcal{C}$. It has an $\mathbb{R}$-basis consisting of K matrices, $1 \leq K \leq 2n^2$, so that each matrix X in $\mathcal{C}$ can be uniquely written as

$$X = \sum_{i=1}^{K} g_i B_i, \qquad (1)$$

where B_i are some basis matrices and g_i are real numbers. Once the basis matrices $\{B_1, \ldots, B_K\}$ are given, a space-time code $\mathcal{C}$ is defined by the values that g_i, $i = 1, \ldots, K$, can take. We write

$$\mathbf{g} = (g_1, \ldots, g_K)$$

and let $\mathbf{g}$ take its values in $\mathcal{G} \subseteq \mathbb{R}^K$, so that

$$\mathcal{C} = \{\sum_{i=1}^{K} g_i B_i \,|\, \mathbf{g} = (g_1, \ldots, g_K) \in \mathcal{G}\ \}. \qquad (2)$$

Typically, $\mathcal{G}$ corresponds to a choice of constellation points. For example, if a size Q pulse amplitude modulation (Q-PAM) is used, then $\mathcal{G}$ is the Cartesian product of K times

$$\{-Q+1,\dots,-3,-1,1,3,\dots,Q-1\},$$

where $Q \geq 2, 2|Q$. The formulation in (2) is not without recalling the notion of *linear dispersion codes* [17], where codewords X are similarly described by a family of dispersion matrices $\{A_1,\dots,A_K\}$: $X = \sum_{i=1}^{K} g_i A_i$, for some coefficients g_i belonging to a symmetric set. The critical difference is in $\{B_1,\dots,B_K\}$ being linearly independent, and thus really forming an $\mathbb{R}$-basis for $\langle\mathcal{C}\rangle$. It consequently makes sense to speak of dimension of $\langle\mathcal{C}\rangle$, which yields the following definition of rate [15]:

Definition 2.2: The *dimension rate* R_1 of the code $\mathcal{C}$ is given by

$$R_1 = \frac{\dim_{\mathbb{R}}(\langle\mathcal{C}\rangle)}{n} = \frac{K}{n}$$

(real) dimensions per channel use.

Since $1 \leq K \leq 2n^2$, we immediately see that the maximum rate achievable for square matrices is $2n$. One should note that this is not the common definition of a *code rate* (also used in this paper until now), which usually counts how many complex symbols (*e.g.* QAM symbols) are transmitted in a codeword. With our notation, the common code rate would be $R_1/2 \leq n$.

The data rate in bits per channel use (bpcu) is defined as follows.

Definition 2.3: The *bit rate* R_2 of the code $\mathcal{C}$ is

$$R_2 = \frac{\log_2(|\mathcal{C}|)}{n}$$

bpcu.

While the above considerations have been done in full generality, several years of research on space-time coding have shown that good space-time codes enjoy special properties. Following [18], getting fully diverse codes has become the first code design criterion. That is, we require

$$\det(X - X') \neq 0,\ X \neq X' \in \mathcal{C}. \tag{3}$$

From [19] it is known that the best way to actually deal with this constraint is to first assume that the space-time code considered forms an additive group, so that

$$X \pm X' \in \mathcal{C}, \tag{4}$$

which simplifies (3) to

$$\det(X) \neq 0,\ X \neq \mathbf{0},$$

a much more tractable constraint. We note that $\mathcal{C}$ as defined in (2) is not necessarily linear, but of course $\langle\mathcal{C}\rangle$ is. From the linearity imposed on $\mathcal{C}$ by (4), we are only one step away from having a *space-time lattice code*. Recall that

Proposition 2.1: An infinite discrete group of matrices in $M_n(\mathbb{C})$ is a lattice.

We can thus safely assume that infinite space-time codes have a lattice structure, since the discreteness condition can be translated by asking the Euclidean distance between each pair of codewords to be greater than r, for a fixed non-zero r. This formalizes the natural assumption that codewords should not be chosen too close to each other.

Definition 2.4: A *space-time lattice code* $\mathcal{C} \subseteq M_n(\mathbb{C})$ has the form

$$\mathbb{Z}B_1 \oplus \mathbb{Z}B_2 \cdots \oplus \mathbb{Z}B_K,$$

where the matrices $B_1,\dots,B_K$ are linearly independent, *i.e.*, form a lattice basis, and K is called the *rank* of the lattice. We may also call K the *dimension* of the code, but do not confuse this with the dimension of the lattice.

For the actual transmission, a finite subset of codewords from $\mathcal{C}$ is picked by restricting the integer coefficients to some set $\mathcal{G}$, as in (2). From now on, we will consider only space-time lattice codes and may call them space-time codes for short.

As recalled above, full diversity is the first design criterion for space-time codes. Once achieved, meaning for lattice codes that

$$\det(X) \neq 0,\ X \neq \mathbf{0},$$

the next criterion is to maximize the minimum determinant of the code.

Definition 2.5: The *minimum determinant* $\det_{min}(\mathcal{C})$ of a space-time code $\mathcal{C} \subset M_n(\mathbb{C})$ is defined to be

$$\det_{min}(\mathcal{C}) = \inf_{X \neq \mathbf{0}} |\det(X)|,\ X \in \mathcal{C}.$$

Definition 2.6: [20] If the minimum determinant of the lattice is non-zero, we say that the code has a *non-vanishing determinant* (NVD) .

The NVD property means that, prior to SNR normalization, the lower bound on the minimum determinant does not depend on the size of the constellation used.

B. Sphere decoding

Let X be a space-time lattice codeword. We can flatten $X \in M_n(\mathbb{C})$ to obtain a $2n^2$-dimensional real vector $\mathbf{x}$ by first forming a vector of length n^2 out of the entries (*e.g.* row by row, or vectorizing that is column by column) and then replacing each complex entry with the pair formed by its real and imaginary parts. This defines a mapping α from $M_n(\mathbb{C})$ to $\mathbb{R}^{2n^2}$:

$$\alpha : X \mapsto \mathbf{x} = \alpha(X) \tag{5}$$

which is clearly $\mathbb{R}$-linear:

$$\alpha(rX + r'X') = r\alpha(X) + r'\alpha(X'),\ r, r' \in \mathbb{R}. \tag{6}$$

Let $||X||_F = \sqrt{\mathrm{Tr}(X^\dagger X)}$ denote the Frobenius norm of X. Note that the following equality holds:

$$||X||_F = \sqrt{\sum_{i=1}^{n}\sum_{j=1}^{n} |x_{ij}|^2} = ||\alpha(X)||_E, \tag{7}$$

where $|| \cdot ||_E$ denotes the Euclidean norm of a vector. This makes α an isometry.

The space-time code $X \in M_n(\mathbb{C})$ is transmitted over a coherent Rayleigh fading channel with perfect channel state information at the receiver (CSIR):

$$Y = HX + V,$$

where H is the channel matrix and V is the Gaussian noise at the receiver. Maximum-likelihood (ML) decoding consists of finding the codeword X that achieves the minimum of the squared Frobenius norm

$$d(X) = ||Y - HX||_F^2. \tag{8}$$

This search can be performed using a real sphere decoder (see *e.g.* [21]). Since this paper focuses on MIDO codes and for the sake of simplicity, we will now exemplify the computation of a (4×4) MIDO code matrix X, that is, we consider 4 Tx antennas and 2 Rx antennas and the channel

$$Y_{2\times 4} = H_{2\times 4} X_{4\times 4} + V_{2\times 4}. \tag{9}$$

A (4×4) MIDO code can transmit up to 8 complex (say QAM) information symbols, or equivalently 16 real (say PAM) information symbols. Following (2), the encoding can thus be written as mapping the PAM vector

$$\mathbf{g} = (g_1, \ldots, g_{16})^T$$

into a (4×4) matrix

$$X = \sum_{i=1}^{16} g_i B_i,$$

where the basis matrices B_i, $i = 1, \ldots, 16$, define the code. Let us emphasize again that by basis matrices, we really mean a $\mathbb{Z}$-basis of the code seen as a lattice. From (9), the received matrix Y can be expressed as

$$Y_{2\times 4} = H(\sum_{i=1}^{16} g_i B_i) + V = \sum_{i=1}^{16} g_i (HB_i) + V.$$

In order to perform real sphere decoding, we have to transform this complex channel equation into a real one, which can be done via the mapping α defined in (5). The matrix $Y_{2\times 4} = (y_{i,j})$ can be turned into a real valued vector $\mathbf{y}$ in $\mathbb{R}^{16}$ by the transformation

$$\alpha(Y) = \mathbf{y} = [\mathbf{y}_1, \mathbf{y}_2]^T$$

with

$$\begin{array}{l}\mathbf{y}_1 = (\Re(y_{1,1}), \Im(y_{1,1}), \ldots, \Re(y_{1,4}), \Im(y_{1,4}))\\ \mathbf{y}_2 = (\Re(y_{2,1}), \Im(y_{2,1}), \ldots, \Re(y_{2,4}), \Im(y_{2,4})).\end{array}$$

The matrices $HB_i \in M_{4\times 2}(\mathbb{C})$ are then similarly turned into vectors $\mathbf{b}_i \in \mathbb{R}^{16}$:

$$\alpha(HB_i) = \mathbf{b}_i,\ i = 1, \ldots, 16,$$

so that $d(X)$ can be expressed as

$$\begin{array}{rcll} d(X) & = & ||Y - HX||_F^2 & \text{by (8)}\\ & = & ||\alpha(Y - HX)||_E^2 & \text{by (7)}\\ & = & ||\alpha(Y) - \alpha(HX)||_E^2 & \text{by (6)}\\ & = & ||\mathbf{y} - \sum_{i=1}^{16} g_i \mathbf{b}_i||_E^2. & \end{array}$$

From this we finally get

$$d(X) = ||\mathbf{y} - B\mathbf{g}||_E^2, \tag{10}$$

where

$$B = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{16}) \in M_{16\times 16}(\mathbb{R}).$$

This shows that the decoding of a space-time lattice code $\mathcal{C}$ with a basis $\{B_1, \ldots, B_K\}$ is equivalent to the decoding of a 16-dimensional real lattice $\Lambda(\mathcal{C})$ described by the generator matrix B: $\Lambda(\mathcal{C}) = \{\mathbf{x} = B\mathbf{g} \mid \mathbf{g} \in \mathbb{Z}^n\}$.

III. Fast-decodable space-time codes

We are now ready to explain the notion of fast decodability of space-time lattice codes when using sphere decoding. We will then give a few examples that will motivate the rest of the paper.

A. Fast sphere decoding

The first step of the sphere decoder is to perform a QR decomposition of the lattice generator matrix B, $B = QR$, with $Q^\dagger Q = I$, to reduce the computation of

$$d(X) = ||\mathbf{y} - B\mathbf{g}||_E^2$$

as in (10) to

$$d(X) = ||\mathbf{y} - QR\mathbf{g}||_E^2 = ||Q^\dagger \mathbf{y} - R\mathbf{g}||_E^2 \tag{11}$$

where R is an upper right triangular matrix. The number and position of non-zero elements in the upper right part of R will determine the complexity of the sphere decoding process [4], [5].

The worst case is of course given when the matrix R is a full upper right triangular matrix. This motivates the following definition of worst case sphere decoding complexity:

Definition 3.1: [4, Def. 2] Let S denote the real alphabet in use, and let κ be the number of independent real information symbols from S within one code matrix. The *ML decoding complexity* is the minimum number of values of $d(X)$ in (11) that should be computed while performing ML decoding. This number cannot exceed $|S|^{\kappa}$, the complexity of the exhaustive-search ML decoder (or $|S|^{\kappa/2}$ for a complex alphabet S).

Definition 3.2: The exponent κ (resp. $\kappa/2$) is referred to as the *dimension of a real (resp. complex) sphere decoder*. If the structure of the code is such that κ decreases, we say that the code is *fast-decodable*. In this paper, we always refer to the dimension of a real sphere decoder.

In the MIDO case (9), where S is a real PAM alphabet (and hence $|S|$ is the number of PAM symbols in use), the worst case complexity is $|S|^{16}$. A typical improvement in κ can be obtained if the left upper corner of the matrix

$$R = \begin{pmatrix} R^{1,1} & R^{1,2} \\ R^{2,1} & R^{2,2} \end{pmatrix}$$

from the QR decomposition of B has the form

$$R^{1,1} = \begin{pmatrix} \star & \star & \star & \star & 0 & 0 & 0 & 0 \\ 0 & \star & \star & \star & 0 & 0 & 0 & 0 \\ 0 & 0 & \star & \star & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \star & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \star & \star & \star & \star \\ 0 & 0 & 0 & 0 & 0 & \star & \star & \star \\ 0 & 0 & 0 & 0 & 0 & 0 & \star & \star \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \star \end{pmatrix}, \qquad (12)$$

where $\star$ denotes any non-zero element. Indeed, in this case:

1) We start the sphere decoding by going through every combination of the 8 last real symbols $g_9, \dots, g_{16}$ (we are not choosing the ones that give the minimal metric yet, we go through all the options since we do not know how the last 8 symbols will affect the total minimization problem). This corresponds to treating the matrix $R^{2,2}$, and has cost $|S|^8$.
2) We then look at the first 8 symbols $g_1, \dots, g_8$, corresponding to the matrix $R^{1,1}$, and for every possible choice of 8-tuples, $(g_9, \dots, g_{16})$, we decode separately $g_1, \dots, g_4$ and $g_5, \dots, g_8$ thanks to the structure of $R^{1,1}$, which has complexity $2|S|^4$.

Altogether, the above structure allows to decode the PAM symbols g_1, g_2, g_3, g_4 independently of the symbols $g_9, g_{10}, g_{11}, g_{12}$, yielding a worst case complexity of $|S|^{12}$ (or more precisely $2|S|^{12}$) for the real sphere decoding process instead of the full complexity order of $|S|^{16}$.

The natural question to ask is thus the design of codes (that is, of the basis matrices B_i) that yield a sparse matrix R. To address this question, we further study the structure of the matrix R. By definition of the QR decomposition of the matrix $B = (\mathbf{b}_1, \dots, \mathbf{b}_{16})$, we have that

$$R = \begin{pmatrix} \langle \mathbf{e}_1, \mathbf{b}_1 \rangle & \langle \mathbf{e}_1, \mathbf{b}_2 \rangle & \dots & \langle \mathbf{e}_1, \mathbf{b}_{16} \rangle \\ 0 & \langle \mathbf{e}_2, \mathbf{b}_2 \rangle & \dots & \langle \mathbf{e}_2, \mathbf{b}_{16} \rangle \\ 0 & 0 & & \langle \mathbf{e}_3, \mathbf{b}_{16} \rangle \\ 0 & 0 & \ddots & \vdots \\ 0 & 0 & & \langle \mathbf{e}_{16}, \mathbf{b}_{16} \rangle \end{pmatrix}$$

where

$$\begin{aligned} \mathbf{e}_1 &= \frac{\mathbf{b}_1}{||\mathbf{b}_1||} \\ \mathbf{e}_2 &= \frac{\mathbf{b}_2 - \mathrm{proj}_{\mathbf{e}_1}\mathbf{b}_2}{||\mathbf{b}_2 - \mathrm{proj}_{\mathbf{e}_1}\mathbf{b}_2||} \\ &\vdots \\ \mathbf{e}_k &= \frac{\mathbf{b}_k - \sum_{j=1}^{k-1}\mathrm{proj}_{\mathbf{e}_j}\mathbf{b}_j}{||\mathbf{b}_k - \sum_{j=1}^{k-1}\mathrm{proj}_{\mathbf{e}_j}\mathbf{b}_j||} \end{aligned}$$

and

$$\mathrm{proj}_{\mathbf{e}}\mathbf{b} = \frac{\langle \mathbf{e}, \mathbf{b} \rangle}{\langle \mathbf{e}, \mathbf{e} \rangle}\mathbf{e}.$$

The notation $\langle \cdot, \cdot \rangle$ stands for the usual inner product. Thus having the upper left part of R to look like (12) means that

$$\langle \mathbf{b}_i, \mathbf{b}_j \rangle = 0,\ 1 \le i \le 4,\ 5 \le j \le 8,$$

or equivalently, by recalling that $\mathbf{b}_i = \alpha(HB_i)$

$$0 = \langle \alpha(HB_i), \alpha(HB_j) \rangle = \Re(\mathrm{Tr}(HB_i(HB_j)^\dagger)).$$

The second equality is true in general and can be shown by a direct computation:

$$\langle \alpha(A), \alpha(B) \rangle = \Re(\mathrm{Tr}(AB^\dagger)). \qquad (13)$$

We have now connected the decoding complexity to the code design. The above computations showed that if the 16 basis matrices $B_1, \dots, B_{16}$ satisfy

$$0 = \Re(\mathrm{Tr}(HB_i(HB_j)^\dagger)),\ 1 \le i \le 4,\ 5 \le j \le 8,$$

the worst case sphere decoding complexity is of the order of $|S|^{12}$. This suggests further improvement: the current process manages to separate the information symbols into two groups, which could be repeated. Assume that we could further have

$$0 = \Re(\mathrm{Tr}(HB_i(HB_j)^\dagger)),\ 1 \le i \le 2,\ 3 \le j \le 4$$

and

$$0 = \Re(\mathrm{Tr}(HB_i(HB_j)^\dagger)),\ 5 \le i \le 6,\ 7 \le j \le 8.$$

3) As earlier, we start the sphere decoding with the matrix $R^{2,2}$ and go through all the possibilites for the 8 last real symbols $g_9, \dots, g_{16}$, for a cost of $|S|^8$.
4) For the first 8 symbols $g_1, \dots, g_8$ corresponding to the matrix $R^{1,1}$, we first separate $g_1, \dots, g_4$ and $g_5, \dots, g_8$, after which we decode independently $\{g_1, g_2\}$, $\{g_3, g_4\}$, $\{g_5, g_6\}$ and $\{g_7, g_8\}$, each of these costing $|S|^2$.

The worst case complexity is then $4|S|^8|S|^2 = 4|S|^{10}$.

Remark 3.1: It is possible to further reduce the (ML) complexity by using the so-called *hard-limiting*, see [5, Section VI, p. 924 (1-2)]. In this case, the complexity will be $4|S|^{4.5}$, where $|S|$ is the size of a complex signal constellation. However, this is only possible when a square constellation (*e.g.* Q^2-QAM) can be employed, *i.e.*, the constellation is a cartesian product of two real constellations (*e.g.* Q-PAM).

B. Examples from the ring of Hamiltonian quaternions

To illustrate the material explained above, let us start with the Alamouti code [6], *i.e.*, codewords of the form

$$X = \begin{pmatrix} x_1 & -x_2^* \\ x_2 & x_1^* \end{pmatrix} = \begin{pmatrix} g_1 + ig_2 & -g_3 + ig_4 \\ g_3 + ig_4 & g_1 - ig_2 \end{pmatrix},$$

where x_1, x_2 are QAM symbols and $\mathbf{g} = (g_1, g_2, g_3, g_4)$ is the PAM symbol vector. A decomposition into basis matrices B_1, B_2, B_3, B_4 is given by

$$X = g_1B_1 + g_2B_2 + g_3B_3 + g_4B_4,$$

where

$$B_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ B_2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

$$B_3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ B_4 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

We assume transmission through a MISO channel described by the vector

$$H = (h_1, h_2)$$

so that $\alpha(HB_i)$, $i = 1, 2, 3, 4$, is given by

$$\begin{aligned} \mathbf{b}_1 = \alpha(HB_1) &= (\Re(h_1), \Im(h_1), \Re(h_2), \Im(h_2))^T, \\ \mathbf{b}_2 = \alpha(HB_2) &= (-\Im(h_1), \Re(h_1), \Im(h_2), -\Re(h_2))^T, \\ \mathbf{b}_3 = \alpha(HB_3) &= (\Re(h_2), \Im(h_2), -\Re(h_1), -\Im(h_1))^T, \\ \mathbf{b}_4 = \alpha(HB_4) &= (-\Im(h_2), \Re(h_2), -\Im(h_1), \Re(h_1))^T. \end{aligned}$$

We finally get

$$B = \alpha(HX) = [\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4],$$

and since $\langle \mathbf{b}_i, \mathbf{b}_j \rangle = 0$ for $i \neq j$, the QR decomposition of B is of the form

$$B = \left(\frac{1}{c}B\right)(cI_4) = QR,$$

where

$$c = \sqrt{\Re(h_1)^2 + \Im(h_1)^2 + \Re(h_2)^2 + \Im(h_2)^2}$$

is a normalization factor which makes Q orthonormal. The matrix R is indeed upper right triangular, with in fact only zeroes above its diagonal. Thus the worst case decoding complexity of such a code is the size of the QAM alphabet, that is, of linear order.

Finding basis matrices with similar properties as those of the Alamouti code seems a difficult task. The question is in general to find families of matrices $\{B_1, \dots, B_K\}$ which are *orthogonal* in the sense that $\langle \alpha(B_i), \alpha(B_j) \rangle = 0$, $i \neq j$, and will keep this property even after multiplication by an arbitrary channel matrix H. Let us start modestly and wonder whether we could find such a pair of matrices $B, B' \in M_n(\mathbb{C})$ whose orthogonality will resist a channel matrix $H \in M_{k \times n}(\mathbb{C})$, where $n \ge k$. Using (13), we need to check that

$$0 = \langle \alpha(HB), \alpha(HB') \rangle = \Re(\mathrm{Tr}(HB(HB')^\dagger)).$$

As a first example, take

$$B = \begin{pmatrix} x_1 & 0 \\ 0 & x_1^* \end{pmatrix} \text{ and } B' = \begin{pmatrix} 0 & -x_2^* \\ x_2 & 0 \end{pmatrix},$$

where $x_1, x_2 \in \mathbb{C}$. These two matrices clearly satisfy the orthogonality relation $\langle \alpha(B), \alpha(B') \rangle = 0$. Now pick an arbitrary complex matrix

$$H = \begin{pmatrix} h_1 & h_2 \\ h_3 & h_4 \end{pmatrix}.$$

A direct calculation shows that

$$\begin{aligned} & \mathrm{Tr}(HB(HB')^\dagger) \\ = \ & x_1h_1x_2^*h_2^* - h_2x_2h_1^*x_1^* + x_1h_3x_2^*h_4^* - x_2h_4h_3^*x_1^* \\ = \ & i\Im(x_1h_1x_2^*h_2^*) + i\Im(x_1h_3x_2^*h_4^*) \end{aligned}$$

so that

$$\Re(\mathrm{Tr}(HB(HB')^\dagger)) = 0,$$

independently of the matrix H.

As a second example, consider

$$B = \begin{pmatrix} x_1 & 0 & 0 & 0 \\ 0 & x_1* & 0 & 0 \\ 0 & 0 & x_3 & 0 \\ 0 & 0 & 0 & x_3* \end{pmatrix},$$

$$B' = \begin{pmatrix} 0 & -x_2* & 0 & 0 \\ x_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -x_4* \\ 0 & 0 & x_4 & 0 \end{pmatrix}$$

and

$$H = \begin{pmatrix} h_1 & h_2 & h_3 & h_4 \\ h_5 & h_6 & h_7 & h_8 \end{pmatrix}.$$

We can similarly see that $\Re(\mathrm{Tr}(HB(HB')^\dagger)) = 0$.

The notable thing however is that both examples are closely related to the Alamouti code (the first example being really included in it). This is not a surprise, since most of the work available on fast ML decodability tries to actually exploit the code structure. To pursue our investigation on fast decodability, we now need to focus on algebraic constructions of space-time lattice codes from division algebras.

IV. Space-time codes from division algebras

A. Background

Since the work of Sethuraman et al. [19], a standard algebraic technique to build space-time block codes is to use cyclic division algebras over number fields (that is, finite extensions of the field $\mathbb{Q}$). For the sake of completeness, we will start by recalling the formal definition of a cyclic algebra, after which we will provide an illustrative example, rather than redo the whole theory, which the reader can find in [19], or in the tutorial [22].

Definition 4.1: Let K be an algebraic number field and assume that E/K is a cyclic Galois extension of degree n with Galois group $\mathrm{Gal}(E/K) = \langle\sigma\rangle$. We can now define an associative K-algebra

$$\mathcal{A} = (E/K, \sigma, \gamma) = E \oplus uE \oplus u^2E \oplus \cdots \oplus u^{n-1}E,$$

where $u \in \mathcal{A}$ is an auxiliary generating element subject to the relations $xu = u\sigma(x)$ for all $x \in E$ and $u^n = \gamma \in K^*$, where K^* denotes K without the zero element.

The element γ is often called a *non-norm* element due to its relation to the invertibility of the elements of $\mathcal{A}$. Namely, if there exists no element $x \in E$ such that its norm would be $\mathcal{N}_{E/K}(x) = \gamma^t$, where $t \in \mathbb{Z}_+$ is a proper divisor of n, then $\mathcal{A}$ will be a division algebra [23, Prop. 2.4.5]. This result is a straightforward simplification of a theorem by Albert [24].

Space-time codewords are obtained by considering matrices of left multiplication by an element of $\mathcal{A}$ in the above basis.

Let us see how the coding is done more concretely through an example. We first need a number field E of degree n whose Galois group is cyclic. For example, take $\zeta_5 = e^{2i\pi/5}$ a primitive 5th root of unity, and consider the number field $E = \mathbb{Q}(i, \zeta_5)$ over $K = \mathbb{Q}(i)$, given by

$$\mathbb{Q}(i, \zeta_5) = \{x = a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3,\ a, b, c, d \in \mathbb{Q}(i)\}.$$

It is of degree 4 (*i.e.*, of dimension 4 as a vector space) over $\mathbb{Q}(i)$. Let us assume that we want to encode QAM symbols. Since they can be seen as elements in $\mathbb{Z}[i] \subset \mathbb{Q}(i)$, we have that one element x in $\mathbb{Q}(i, \zeta_5)$ encodes 4 QAM symbols, namely a, b, c, d, as linear combinations in the given basis. The Galois group of $\mathbb{Q}(i, \zeta_5)/\mathbb{Q}(i)$ describes maps that permute ζ_5 and its conjugates ζ_5^j, $j = 2, 3, 4$ while fixing $\mathbb{Q}(i)$. If $\sigma(\zeta_5) = \zeta_5^2$, we have that

$$\sigma^2(\zeta_5) = \zeta_5^4,\ \sigma^3(\zeta_5) = \zeta_5^3,\ \sigma^4(\zeta_5) = \zeta_5$$

yielding a cyclic Galois group. We now build an associative algebra $\mathcal{A}$ based on E. As a vector space, $\mathcal{A}$ can be seen as a sum of n copies of the chosen number field E of degree n. In our example, this gives

$$\mathcal{A} = \mathbb{Q}(i, \zeta_5) \oplus u\mathbb{Q}(i, \zeta_5) \oplus u^2\mathbb{Q}(i, \zeta_5) \oplus u^3\mathbb{Q}(i, \zeta_5)$$

where $\{1, u, u^2, u^3\}$ forms a basis and $\gamma = u^4$ must be an element of the base field $\mathbb{Q}(i)$, say $u^4 = i$. A space-time block code can be obtained by considering the matrix of left multiplication in this given basis. If $x = x_0 + ux_1 + u^2x_2 + u^3x_3 \in \mathcal{A},\ x_0, x_1, x_2, x_3 \in \mathbb{Q}(i, \zeta_5)$, then its corresponding multiplication matrix is

$$X = \begin{pmatrix} x_0 & i\sigma(x_3) & i\sigma^2(x_2) & i\sigma^3(x_1) \\ x_1 & \sigma(x_0) & i\sigma^2(x_3) & i\sigma^3(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & i\sigma^3(x_3) \\ x_3 & \sigma(x_2) & \sigma^2(x_1) & \sigma^3(x_0) \end{pmatrix} \quad (14)$$

where the factor i comes from $u^4 = i$ and σ^j, $j = 1, 2, 3, 4$, are the elements of the Galois group, appearing due to the non-commutative multiplication defined on $\mathcal{A}$ by $xu = u\sigma(x)$ for $x \in E$.

Let $\mathcal{C}$ be the codebook formed by codewords X of the above form. For it to be fully diverse, recall from (3) that it is enough to have

$$\det(X' - X'') \neq 0$$

for $X' \neq X''$ in $\mathcal{C}$, or equivalently, by linearity since we are considering space-time lattice codes

$$\det(X) \neq 0$$

for $X \neq \mathbf{0}$ in $\mathcal{C}$. This can be obtained by asking for $\mathcal{A}$ to be a division algebra, property that depends on the choice of the value of γ (or $\gamma = i$ in our example). If there exists no element $a \in \mathbb{Q}(i, \zeta_5)$ such that its norm is i or i^2, *i.e.*, $\mathcal{N}_{\mathbb{Q}(i,\zeta_5)/\mathbb{Q}(i)}(a) = i$, or -1, then $\mathcal{A}$ will be a division algebra [24], [23].

Let us check that $\mathcal{A}$ is indeed a division algebra. Note for this purpose that $\mathbb{Q}(\zeta_5+\zeta_5^{-1})=\mathbb{Q}(\sqrt{5})$ is a subfield of $\mathbb{Q}(\zeta_5)$. Suppose now that there exists an element $a \in E$ such that $\mathcal{N}_{\mathbb{Q}(i,\zeta_5)/\mathbb{Q}(i)}(a)=i$, then, by transitivity of the norm

$$\mathcal{N}_{\mathbb{Q}(i,\zeta_5)/\mathbb{Q}(i)}(a)=\mathcal{N}_{\mathbb{Q}(i,\sqrt{5})/\mathbb{Q}(i)}\mathcal{N}_{\mathbb{Q}(i,\zeta_5)/\mathbb{Q}(i,\sqrt{5})}(a)=i,$$

which implies the existence of an element $b = \mathcal{N}_{\mathbb{Q}(i,\zeta_5)/\mathbb{Q}(i,\sqrt{5})}(a)$ such that

$$\mathcal{N}_{\mathbb{Q}(i,\sqrt{5})/\mathbb{Q}(i)}(b)=i,$$

a contradiction [25].

The case of a norm of -1 is tougher though. However, there are several ways to deal with it. We refer the reader to [16, Section 8], where the proof used for the algebra D_4 can be used here verbatim.

We have thus constructed in our example a fully-diverse (4×4) space-time code matrix. It furthermore has the non-vanishing determinant property (see Definition 2.6), since the information symbols are restricted to algebraic integers in L, and hence the minimum determinant belongs to $\mathbb{Z}[i]$, yielding $\min_{X\neq\mathbf{0}}|\det(X)|=1$ (cf. [16]).

We conclude with two important invariants of central simple algebras. Central simple K-algebras are algebras whose center is K and which have only trivial two-sided ideals. Cyclic algebras are particular cases of central simple algebras. We could have stated these definitions only for cyclic algebras, but for the rest of this work, we will need them in more generality.

Definition 4.2: Let $\mathcal{A}$ be a central simple K-algebra. The *degree* of $\mathcal{A}$ is the integer $\deg(\mathcal{A})=\sqrt{\dim_K(\mathcal{A})}$.

Wedderburn's theorem is a major theorem in the theory of central simple algebras, which tells that every central simple algebra (and thus in particular every cyclic algebra) is isomorphic to a matrix algebra over a central division K-algebra $\mathcal{D}$.

Definition 4.3: The *index* of $\mathcal{A}$ is the integer $\mathrm{ind}(\mathcal{A})=\deg(\mathcal{D})$ where $\mathcal{D}$ is the unique central division K-algebra associated to $\mathcal{A}$ by Wedderburn's theorem.

We have that $\mathrm{ind}(\mathcal{A}) \mid \deg(\mathcal{A})$ and equality holds if and only if $\mathcal{A}$ is a division algebra.

B. Examples

Let us now consider a few well known examples of division algebra codes, and see how they behave with respect to fast decodability.

The Alamouti code [6] can be seen from an algebraic perspective as a cyclic division algebra

$$\mathcal{D}_{Alam}=(\mathbb{Q}(i)/\mathbb{Q},\sigma,-1), \qquad (15)$$

where σ is the complex conjugation. This is a $\mathbb{Q}$-central division algebra of index 2, whose cyclic representation indeed yields codewords of the type

$$\begin{pmatrix} x_1 & -x_2^* \\ x_2 & x_1^* \end{pmatrix},$$

where x_i are in $\mathbb{Z}[i]$ (that is, they are QAM symbols).

This algebra is more commonly known as the Hamiltonian quaternions

$$\mathbf{H}=\{a+ib+jc+ijd \mid a,b,c,d\in\mathbb{R}\},$$

$$\text{where } i^2=j^2=-1,\ ij=-ji.$$

Probably the most important property of this code is that, when used over a MISO channel, its worst case decoding complexity is linear, as was shown in Subsection III-B.

Let us now consider the division algebra

$$\mathcal{D}_{ort}=(\mathbb{Q}(i,\sqrt{2})/\mathbb{Q}(\sqrt{2}),\sigma,-1) \qquad (16)$$

from [7]. This is an index 2 algebra with center $\mathbb{Q}(\sqrt{2})$. It can be turned into a space-time code by mapping the element $x=a_1+a_2\zeta_8+ua_3+u\zeta_8a_4\in\mathcal{D}_{ort}$ to a codeword X given by

$$\begin{pmatrix} a_1+a_2\zeta_8 & -a_3^*-a_4^*\zeta_8^* & 0 & 0 \\ a_3+a_4\zeta_8 & a_1^*+a_2^*\zeta_8^* & 0 & 0 \\ 0 & 0 & a_1-a_2\zeta_8 & -a_3^*+a_4^*\zeta_8^* \\ 0 & 0 & a_3-a_4\zeta_8 & a_1^*-a_2^*\zeta_8^* \end{pmatrix},$$

where $a_j=g_{2j-1}+a_{2j}\in\mathbb{Z}[i]$, $j=1,2,3,4$. We can now write this in the form

$$X=\sum_{j=1}^{8} g_jB_j,$$

where $\mathbf{g}=(g_1,\dots,g_8)$ is the PAM symbol vector, and the basis matrices are

$$B_1=\mathrm{diag}(1,1,1,1),\ B_3=\mathrm{diag}(\zeta_8,\zeta_8^*,-\zeta_8,-\zeta_8^*),$$

$$B_2=\mathrm{diag}(i,-i,i,-i),\ B_4=\mathrm{diag}(i\zeta_8,-i\zeta_8^*,-i\zeta_8,i\zeta_8^*),$$

$$B_5=\begin{pmatrix} 0 & -1 & & \\ 1 & 0 & & \\ & & 0 & -1 \\ & & 1 & 0 \end{pmatrix}, B_7=\begin{pmatrix} 0 & -\zeta_8^* & & \\ \zeta_8 & 0 & & \\ & & 0 & \zeta_8^* \\ & & -\zeta_8 & 0 \end{pmatrix},$$

$$B_6=\begin{pmatrix} 0 & i & & \\ i & 0 & & \\ & & 0 & i \\ & & i & 0 \end{pmatrix}, B_8=\begin{pmatrix} 0 & i\zeta_8^* & & \\ i\zeta_8 & 0 & & \\ & & 0 & -i\zeta_8^* \\ & & -i\zeta_8 & 0 \end{pmatrix}.$$

The decoding complexity of this code for a MISO channel is $2|S|^4$ instead of the maximal complexity

MISO code	matrix	center	index	$\lvert S\rvert^{\kappa}$ (real)	max $\lvert S\rvert^{\kappa}$
$\mathcal{D}_{Alam}$	(2×2)	$\mathbb{Q}$	2	$\lvert S\rvert$	$\lvert S\rvert^4$
$\mathcal{D}_{ort}$	(4×4)	$\mathbb{Q}(\sqrt{2})$	2	$\lvert S\rvert^4$	$\lvert S\rvert^8$
$\mathcal{A}_2$	(2×2)	$\mathbb{Q}$	2	$\lvert S\rvert^4$	$\lvert S\rvert^4$

TABLE I
CODE CONSTRUCTIONS: ALGEBRAIC PROPERTIES VERSUS DECODING COMPLEXITY

$|S|^8$. Indeed, write the channel $H = (h_1, h_2, h_3, h_4)$ as (H_1, H_2) with $H_1 = (h_1, h_2)$ and $H_2 = (h_3, h_4)$, so that

$$HB_i = (H_1, H_2) \begin{pmatrix} B_i^{1,1} & \mathbf{0} \\ \mathbf{0} & B_i^{2,2} \end{pmatrix} = (H_1 B_i^{1,1}, H_2 B_i^{2,2}),$$

whence $\Re(\mathrm{Tr}(HB_i(HB_j)^\dagger))$ simplifies to

$$\Re(\mathrm{Tr}(H_1 B_i^{1,1}(B_j^{1,1})^\dagger H_1^\dagger) + \mathrm{Tr}(H_2 B_i^{2,2}(B_j^{2,2})^\dagger H_2^\dagger)).$$

The basis matrices are closely related to those of the Alamouti code given in Subsection III-B, and it is easy, using the known orthogonality relations of the Alamouti basis matrices, to see that

$$\Re(\mathrm{Tr}(HB_i(HB_j)^\dagger)) = 0, \ \ i = 1, 2, 3, 4, \ \ j = 5, 6, 7, 8,$$

yielding an upper triangular matrix R of the same form as in (12), and consequently a decoding complexity of $2|S|^4$.

Our final example is the division algebra

$$\mathcal{A}_2 = (\mathbb{Q}(\sqrt{3})/\mathbb{Q}, \sigma, -1),$$

where $\sigma(\sqrt{3}) = -\sqrt{3}$. This algebra is of index 2 with center $\mathbb{Q}$, and yields codewords of the form

$$\begin{pmatrix} x_1 + x_2\sqrt{3} & -x_3 + x_4\sqrt{3} \\ x_3 + x_4\sqrt{3} & x_1 - x_2\sqrt{3} \end{pmatrix},$$

where $x_i \in \mathbb{Z}$. However, as far as we know there is no existing method to reduce the decoding complexity of this code.

We already observed in Subsection III-B that from the decoding perspective, it might be beneficial for codes to inherit some of the special structure of the Alamouti code. This study of different algebraic code structures seems to concur with the same conclusion, expressed now in algebraic terms as: a code should be a subset of $M_k(\mathbf{H})$ for some k. However, which algebras exactly give fast decodability still seems unclear (see Table I). In the following section, we are going to answer this question.

V. Embedding codes into matrix rings of the Hamiltonian quaternions

We have so far discussed fast decodability of space-time codes via sphere decoding, and through several heuristic examples concluded that codewords in rings $M_k(\mathbf{H})$, for some k and $\mathbf{H}$ the Hamiltonian quaternions, are prone to offer orthogonality relations that induce fast sphere decoding. Therefore our main interest is now to study space-time codes that are subsets of the rings $M_k(\mathbf{H})$. This will be characterized by the ramification of the cyclic algebra over which the space-time code is built.

A. Embedding division algebras into $M_k(\mathbf{H})$

Let $K/\mathbb{Q}$ be an algebraic extension of degree m. We then have that

$$m = r_1 + 2r_2,$$

where r_1 is the number of real embeddings and r_2 the number of pairs of complex embeddings of K. We call these embeddings the *infinite primes* of the field K and the non-zero prime ideals of the ring $\mathcal{O}_K$ the *finite primes* of the field K. If the embedding is complex, resp. real, we call it a *complex* resp. *real* prime. To each prime P, finite or infinite, corresponds a local field K_P, obtained by completion of K with respect to the absolute value induced by P (the same way $\mathbb{R}$ is obtained from $\mathbb{Q}$ by completion with respect to the usual absolute value).

Let $\mathcal{A}$ be a central division K-algebra of index and thus degree n. Consider

$$\mathcal{A}_P = \mathcal{A} \otimes_K K_P$$

a central simple K_P-algebra, which is known to be isomorphic to $M_r(\mathcal{D})$ for some r and some central division K_P-algebra $\mathcal{D}$. We denote by m_P the index of $\mathcal{A}_P$ and call it the *local index* of $\mathcal{A}$ at P. We say that P is ramified in $\mathcal{A}$ if $m_P > 1$

Let us define the space $G(\mathbb{C})_n \subseteq M_{n\times 2n}(\mathbb{C})$ by

$$G(\mathbb{C})_n = \{(B^*, B) \in M_{n\times 2n}(\mathbb{C}) \ |B \in M_n(\mathbb{C})\}$$

and $B^* = (b_{ij}^*)$. Now $\mathcal{A}\otimes_{\mathbb{Q}}\mathbb{R}$ is a semi-simple $\mathbb{Q}$-algebra, and can thus be written as a Cartesian product of simple subalgebras. Its center is $K\otimes_{\mathbb{Q}}\mathbb{R}$, which is isomorphic to copies of $\mathbb{R}$ or $\mathbb{C}$: a copy of $\mathbb{R}$ for each real embedding of K, and one of $\mathbb{C}$ for each pair of conjugate complex embeddings. The simple components of $\mathcal{A}\otimes_{\mathbb{Q}}\mathbb{R}$ will thus have these factors as centers, and will be either central simple algebras over $\mathbb{R}$ or $\mathbb{C}$: those over $\mathbb{C}$ will be matrix algebras over $\mathbb{C}$, while those over $\mathbb{R}$ will be either matrix algebras over $\mathbb{R}$ if $\mathcal{A}$ is not ramified in the corresponding real prime, or matrix algebras over $\mathbf{H}$ if $\mathcal{A}$ is ramified. Formally, we obtain the isomorphism [26]

$$\mathcal{A} \otimes_{\mathbb{Q}} \mathbb{R} \cong M_{n/2}(\mathbf{H})^{\omega} \times M_n(\mathbb{R})^{r_1-\omega} \times G(\mathbb{C})^{r_2}, \quad (17)$$

where ω is the number of real places where $\mathcal{A}$ ramifies. Therefore each element in $\mathcal{A}$ can be seen as a concatenation of ω matrices in $M_n(\mathbb{C})$, $r_1 - \omega$ matrices in $M_n(\mathbb{R})$ and r_2 pairs of conjugate matrices in $M_n(\mathbb{C})$, or alternatively as a matrix in $M_{n\times nm}(\mathbb{C})$, recalling that $m = r_1 + 2r_2$.

The above isomorphism (17) implies an injection ψ

$$\mathcal{A} \hookrightarrow \mathrm{diag}(M_{n/2}(\mathbf{H})^{\omega} \times M_n(\mathbb{R})^{r_1-\omega} \times G(\mathbb{C})^{r_2}), \quad (18)$$

where the diag-operator places the ith $(n \times n)$ block to the ith diagonal block of a matrix in $M_{mn}(\mathbb{C})$. From (18), we now see that it is possible to embed a division algebra $\mathcal{A}$ into $M_k(\mathbf{H})$ if and only if

$$\psi : \mathcal{A} \hookrightarrow \mathrm{diag}(M_{n/2}(\mathbf{H})^{m}), \quad (19)$$

namely we must have $r_2 = 0$ and $r_1 - \omega = 0$. In summary, we have that

Corollary 5.1: In order to be able to embed a division K-algebra $\mathcal{A}$ into $M_{n/2}(\mathbf{H})$:

- The center K cannot have complex places, that is, it must be totally real ($r_1 = m$).
- Combined with the equation $r_1 - \omega = 0$, we then have that $\omega = m$, so that all the infinite places of K must be ramified in $\mathcal{A}$.

Let us then suppose that K is indeed a totally real number field. We shall now give a simple family of cyclic K-algebras that fulfill the second condition above.

Proposition 5.2: Let $\mathcal{A} = (E/K, \sigma, \gamma)$ be a cyclic division algebra, where E is a CM-field (*i.e.*, E is a totally complex field containing a totally real field E_1 such that $[E : E_1] = 2$). Let $\eta_1, \ldots, \eta_m$ be the $\mathbb{Q}$-embeddings of K. If $\eta_i(\gamma)$ is negative for any η_i, then all the infinite places of $\mathcal{A}$ are ramified.

Proof: Let us suppose that P_i is one of the infinite primes in the field K and that η_i is the corresponding $\mathbb{Q}$-embedding. Let k be the smallest possible positive power such that σ^k fixes the totally real subfield E_1 of E. We then have [27, Theorem 30.8]

$$(E/K, \sigma, -\gamma) \otimes_{\mathbb{Q}} K_{P_i} \sim (EK_{P_i}/K_{P_i}, \sigma^k, -\eta_i(\gamma)), \quad (20)$$

where $\sim$ refers to equivalence in the *Brauer group* $B(K_{P_i})$. Because P_i is a real prime, we can identify K_{P_i} and $\mathbb{R}$, and similarly, EK_{P_i} and $\mathbb{C}$, so that from (20), we get $\langle \sigma^k \rangle = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Finally,

$$(E/K, \sigma, -\gamma) \otimes_{\mathbb{Q}} K_{P_i} \sim (\mathbb{C}/\mathbb{R}, \sigma^*, -\eta_i(\gamma)),$$

where σ^* is the complex conjugation and $-\eta_i(\gamma)$ is a negative real number. The claim now follows as $(\mathbb{C}/\mathbb{R}, \sigma^*, -\eta_i(\gamma)) \cong \mathbf{H}$. ■

We point out that for rational numbers r we have $\eta_i(r) = r$. Therefore a negative rational number is always a suitable non-norm element if $\mathcal{A}$ is a division algebra.

Example 5.1: The algebras $\mathcal{D}_{ort}$ and $\mathcal{D}_{Alam}$ discussed above both fulfill the conditions of Proposition 5.2. Therefore $\mathcal{D}_{Alam}$ can be emebdded into $M_1(\mathbf{H}) = \mathbf{H}$ and $\mathcal{D}_{ort}$ into $M_2(\mathbf{H})$.

B. Embedding space-time lattice codes into $M_k(\mathbf{H})$

We have given in Corollary 5.1 the conditions for a division algebra $\mathcal{A}$ of index n to be embedded into $M_{n/2}(\mathbf{H})$. To obtain a space-time lattice code, we need to select a discrete subset of $\mathcal{A}$, namely one of its orders. We denote by $\mathcal{O}_K$ the ring of integers of K, and similarly by $\mathcal{O}_E$ the ring of integers of E.

Definition 5.1: An $\mathcal{O}_K$-order Λ in $\mathcal{A}$ is a subring of $\mathcal{A}$, having the same identity element as $\mathcal{A}$, and such that Λ is a finitely generated module over $\mathcal{O}_K$ and generates $\mathcal{A}$ as a linear space over K.

This choice is motivated by the following example:

Example 5.2: Let E/K be a cyclic extension of algebraic number fields and $(E/K, \sigma, \gamma)$ be a cyclic division algebra, with $\gamma \in K^*$ an algebraic integer. The $\mathcal{O}_K$-module

$$\Lambda = \mathcal{O}_E \oplus u\mathcal{O}_E \oplus \cdots \oplus u^{n-1}\mathcal{O}_E$$

is a subring of the cyclic algebra $(E/K, \sigma, \gamma)$. We refer to this ring as the *natural order* [7]. Most space-time lattice codes built from division algebras [19], [9] have been further restricted to this natural order.

In theoretical considerations we will later mostly consider $\mathcal{O}_K$-orders (where K is the center) but the connection to coding theory is more visible if we consider $\mathcal{O}_K$-orders as $\mathbb{Z}$-modules.

Definition 5.2: A $\mathbb{Z}$-order Λ in $\mathcal{A}$ is a subring of $\mathcal{A}$, having the same identity element as $\mathcal{A}$, and such that Λ is a finitely generated module over $\mathbb{Z}$ and generates $\mathcal{A}$ as a linear space over $\mathbb{Q}$.

The ring $\mathbb{Z}$ is a principal ideal domain and therefore a $\mathbb{Z}$-order is not only finitely generated as a $\mathbb{Z}$-module, but it also has a $\mathbb{Z}$-basis. This basis is also a $\mathbb{Q}$-basis for the algebra $\mathcal{A}$. In particular a $\mathbb{Z}$-basis of an order in $\mathcal{A}$ has $\dim_{\mathbb{Q}}(\mathcal{A})$ elements.

Remark 5.1: The ring $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module. It is also known that K is generated as a linear space over $\mathbb{Q}$. These results reveal that any $\mathcal{O}_K$-order is also a $\mathbb{Z}$-order.

Let us again consider a general division algebra $\mathcal{A}$ having a center K, where $[K : \mathbb{Q}] = m$, and let ψ be the embedding of $\mathcal{A}$ defined in (18).

Proposition 5.3: Let Λ be a $\mathbb{Z}$-order of $\mathcal{A}$. Then $\psi(\Lambda)$ is a mn^2 dimensional lattice in $M_{mn}(\mathbb{C})$. If

$$\{a_1, \dots, a_{mn^2}\}$$

is a $\mathbb{Z}$-basis of the order Λ, then

$$\{\psi(a_1), \dots, \psi(a_{mn^2})\}$$

is a $\mathbb{Z}$-basis of the lattice $\psi(\Lambda)$.

For any non-zero element of the order Λ, we have

$$\det_{min}(\psi(\Lambda)) \geq 1.$$

In particular $\psi(\Lambda)$ is a space-time lattice code that has the NVD property (see Definition 2.6) and dimension rate $mn^2/mn = n$.

Proof: The $\mathbb{Z}$-basis of Λ has $\dim_{\mathbb{Q}}(\mathcal{A})$ elements. We have that $\mathcal{A}$ is of index n and thus degree n, so it is of dimension n^2 over the center K. The center K on the other hand is an m-dimensional $\mathbb{Q}$-vector space. Overall we get that $\dim_{\mathbb{Q}}(\mathcal{A}) = mn^2$. Let us now consider a $\mathbb{Z}$-basis $\{a_1, \dots, a_{mn^2}\}$ of Λ. While it is clear that the set $\{\psi(a_1), \dots, \psi(a_{mn^2})\}$ does generate $\psi(\Lambda)$, it is not directly obvious that $\psi(a_1), \dots, \psi(a_{mn^2})$ are linearly independent over $\mathbb{R}$. For this result and for the claim on $\det_{min}(\psi(\Lambda))$, we refer the reader to [26].

According to Definition 2.2, the dimension rate R_1 for the code $\psi(\Lambda)$ is given by

$$R_1 = \frac{\dim_{\mathbb{R}}(\psi(\Lambda))}{nm} = \frac{mn^2}{nm} = n$$

dimensions per channel use. ■

Remark 5.2: Due to the above connection between an order and a lattice, we may equally call a lattice code an *order code*.

If we now concentrate on codes that are embeddable into $M_k(\mathbf{H})$, we need to restrict to a K-central division algebra $\mathcal{A}$ of index n, where K is totally real and all the infinite places are ramified. We then get from (19) an embedding

$$\psi : \mathcal{A} \hookrightarrow \operatorname{diag}(M_{n/2}(\mathbf{H})^m) \subset \operatorname{diag}(M_n(\mathbb{C})^m).$$

By taking an order $\Lambda \subset \mathcal{A}$, we get a lattice code

$$\psi(\Lambda) = \mathbb{Z}A_1 \oplus \cdots \oplus \mathbb{Z}A_{mn^2} \subset M_{nm}(\mathbb{C}),$$

where $A_i \in M_{nm/2}(\mathbf{H})$, $i = 1, \dots mn^2$, forms a $\mathbb{Z}$-basis of the lattice. Its dimension rate is similarly n. It is clear that forcing a space-time code to be embedded in $M_{n/2}(\mathbf{H})$ imposes an extra constraint. The next result characterizes this constraint in terms of the dimension rate.

Proposition 5.4: Let us suppose that we have a lattice space-time code $\mathcal{C} \subset M_k(\mathbb{C}) \cap M_{k/2}(\mathbf{H})$, where k is even. We then have that

$$\dim_{\mathbb{R}}(\mathcal{C}) \leq k^2.$$

Consequently, the dimension rate R_1 of $\mathcal{C}$ as given in Definition 2.2 is at most k.

Proof: We can see that, as a subspace in $M_2(\mathbb{C})$, the ring of Hamiltonian quaternions has degree 4. Each matrix in $M_{k/2}(\mathbf{H})$ consist of $(k/2)^2$ freely chosen (2×2) blocks that have the inner structure of Hamiltonian quaternions. Therefore we have

$$\dim_{\mathbb{R}}(M_{k/2}(\mathbf{H})) = 4\left(\frac{k}{2}\right)^2 = k^2.$$

■

If we compare the rate n of $\psi(\Lambda)$ with this result, we get n versus nm, where $m = [K : \mathbb{Q}]$. There is thus a trade-off between fast decodability and rate. However, by choosing the center of the algebra $\mathcal{A}$ to be $\mathbb{Q}$, we can meet the optimal dimension rate of Proposition 5.4.

Remark 5.3: We warn the reader here. The theory developed so far is not explicit in a sense that while it does give us a good description of how to construct the needed division algebras (see Proposition 5.2), we have not given an explicit method to produce the embedding (18). In particular, we have no guarantee that the left regular representation would have anything to do with the embedding (18). In Section VII and the following parts of the paper, we will show that there are methods to overcome this problem and that the left regular representation can work as a good starting point.

VI. Bounds and existence results for matrix lattices in $M_k(\mathbf{H})$

So far, we have given conditions for a division central K-algebra $\mathcal{A}$ to be embedded into $M_k(\mathbf{H})$ and shown how to obtain fast-decodable space-time lattice codes from orders of $\mathcal{A}$. In this section we are going to give bounds and existence results for such codes, taking into account an extra code design criterion, namely the normalized minimum determinant of a lattice code.

A. Normalized minimum determinant of an order code

The minimum determinant $\det_{min}(\mathcal{C})$ is a widely used concept to predict the performance of a finite space-time code $\mathcal{C}$, since it determines its coding gain. In order to compare two finite space-time codes $\mathcal{C}_1, \mathcal{C}_2 \in M_n(\mathbb{C})$, one must first check that

- both codebooks have equal number of elements: $|\mathcal{C}_1| = |\mathcal{C}_2|$ and

- both codes are scaled so that the maximum power used is equal: $\max\{||A||_F^2 \,|\, A \in C_1\} = \max\{||B||_F^2 \,|\, B \in C_2\}$.

In the case of infinite lattice codes, due to the discreteness of the set, a non-zero minimum determinant automatically yields the NVD property. Among two NVD codes using the same maximum power, the one with higher minimum determinant will have better coding gain for the infinite lattice, and will thus provide us with a bound on the coding gain of any finite constellation carved from it. Now given an infinite space-time lattice code $\mathcal{C}$, a number R of codewords, and a fixed power constraint, there are different ways to pick a finite constellation that may lead to different coding gains.

The two most typical encoding methods are linear dispersion encoding (cf. the discussion underneath Equation (2)) and spherical encoding. These encoding methods usually result in different constellation shaping, that can be either cubic (more generally orthogonal) shaping, provided the lattice is orthogonal to start with, or spherical shaping. The two possible shapes are described below in more detail.

Spherical shaping. Just as for Gaussian channels, the most energy efficient way to choose codewords from a given lattice is to use spherical shaping. This means that we choose the needed number of lowest energy codewords from the space-time lattice code $\mathcal{C}$ and then scale the finite code $\mathcal{C}(r)$ given by

$$\mathcal{C}(r) = \{\, A \,|\, A \in \mathcal{C}, ||A||_F \leq r\} \subset \mathcal{C} \tag{21}$$

to meet the power constraint, where r depends on the number R of wanted codewords. For large code sizes, this approach will roughly give lattice points inside a K-sphere, where K is the rank of the code lattice (=number of dispersion matrices).

To fairly compare two finite codes $\mathcal{C}_1(r)$ and $\mathcal{C}_2(r)$, one should first scale them so that both the lattices have a fundamental parallelotope of volume 1. Since we consider a space-time lattice code $\mathcal{C} \in M_n(\mathbb{C})$, to define its volume we first map it to $\mathbb{R}^{2n^2}$ via α, yielding the lattice $\alpha(\mathcal{C})$ whose basis is $\{\alpha(B_1), \dots, \alpha(B_K)\}$, obtained from the basis $\{B_1, \dots, B_K\}$ of $\mathcal{C}$. The generator matrix M of $\alpha(\mathcal{C})$ is $M = (\alpha(B_1), \dots, \alpha(B_K))$, where $\alpha(B_i)$ are column vectors, and we define the measure (or volume) $m(\mathcal{C})$ of the fundamental parallelotope of the space-time lattice $\mathcal{C}$ by

$$m(\mathcal{C})^2 = \det(MM^T) = \det(\Big(\Re\mathrm{Tr}(B_i B_j^\dagger)\Big)_{1\leq i,j\leq K}.$$

To combine the notion of minimum determinant with that of scaling the volume of the lattice to evaluate the performance of finite constellations, we use the notion of *normalized minimum determinant* $\delta(\mathcal{C})$, obtained by first scaling the lattice $\mathcal{C}$ to have a unit size fundamental parallelotope and then taking the minimum determinant of the resulting scaled lattice. A simple computation proves the following.

Lemma 6.1: Let $\mathcal{C}$ be a K-dimensional space-time lattice in $M_n(\mathbb{C})$. We then have that

$$\delta(\mathcal{C}) = \det_{min}(\mathcal{C})\,/(m(\mathcal{C}))^{n/K}.$$

The normalized minimum determinant predicts which lattice is likely to produce the finite codes with the biggest minimum determinants, while using spherical shaping.

Cubic shaping. We also consider another kind of shaping, called cubic or orthogonal shaping.

Definition 6.1: We say that a space-time lattice $\mathcal{C}$ in $M_n(\mathbb{C})$ is orthogonal or rectangular if the corresponding real lattice $\alpha(\mathcal{C})$ has a basis that is orthogonal according to the normal inner product of the space $\mathbb{R}^{2n^2}$. If each of of the basis vectors are of equal length, we say that $\mathcal{C}$ is orthonormal.

When the lattice is orthogonal, there is no point of employing spherical shaping (21), for we get the same result by using simple linear dispersion encoding (see the remark in the end of this section) as described after Equation (2).

One can get bounds for the normalized minimum determinant also in the case of cubic shaping, as for example:

Proposition 6.2: [28] Let us suppose that $\mathcal{C}$ is an orthogonally shaped 16-dimensional space-time lattice code in $M_4(\mathbb{C})$. We then have that

$$\delta(\mathcal{C}) \leq \frac{1}{16} = 0.0625.$$

In the particular case where $\mathcal{C}$ is an order code, that is $\mathcal{C} = \psi(\Lambda)$, with Λ an order of an index n division algebra $\mathcal{A} = (E/K, \sigma, \gamma)$ and $[K : \mathbb{Q}] = m$, we know from Proposition 5.3 that $\psi(\Lambda)$ is an mn^2-dimensional lattice in $M_{mn}(\mathbb{C})$ with $\det_{min}(\psi(\Lambda)) = 1$, so that

$$\delta(\psi(\Lambda)) = 1/(m(\mathcal{C}))^{1/n}$$

and the normalized minimum determinant only depends on the volume of the fundamental parallelotope of the order code.

Remark 6.1: Note that the fact whether one uses linear dispersion encoding (i.e., a symmetric coefficient set) or spherical shaping (i.e., an optimized coefficient set) has nothing to do with the shape of the original lattice. Even though the lattice is not orthogonal, we can employ both encoding methods. If the lattice is not badly skewed, then the difference between the two methods is usually not very big, whereas for highly skewed lattices one may see a gap of several dBs.

For orthogonal lattices, both methods will give the same result, provided that the target constellation size is suitable for a symmetric coefficient set to start with.

B. Bounds and existence results

Since the normalized minimum determinant of an order code only depends on the volume of its fundamental parallelotope, one may wonder whether, given a center K, it is possible to find the smallest volume an order inside any division algebra of a given index n can have.

To answer this question, we first further characterize the volume of the order by connecting it to an invariant of the order.

Proposition 6.3: [26] Let Λ be a $\mathbb{Z}$-order in $\mathcal{A}$ and let ψ be the embedding (18). We then have that

$$m(\psi(\Lambda)) = \sqrt{|d(\Lambda/\mathbb{Z})|},$$

where $d(\Lambda/\mathbb{Z})$ is the $\mathbb{Z}$-discriminant of the order Λ (see [27], [16] for an exact definition), and further that

$$\delta(\psi(\Lambda)) = \left(\frac{1}{|d(\Lambda/\mathbb{Z})|}\right)^{1/2n}.$$

Clearly the smaller the absolute value of the $\mathbb{Z}$-discriminant of an order is, the greater the normalized minimum determinant will be.

Inside a given algebra the $\mathbb{Z}$-orders having the smallest possible discriminant are called *maximal orders*. All the maximal orders of a given division algebra share the same discriminant.

While each $\mathcal{O}_K$-order is also $\mathbb{Z}$-order, the opposite does not have to be true. However if a $\mathbb{Z}$-order Λ also is an $\mathcal{O}_K$-module, it is an $\mathcal{O}_K$-order and its $\mathcal{O}_K$-discriminant $d(\Lambda/\mathcal{O}_K)$ is related to its $\mathbb{Z}$-discriminant by the following transitivity formula:

Lemma 6.4: Let $\mathcal{A}$ be a K-central division algebra of index n and let Λ be an $\mathcal{O}_K$-order. If Λ is a $\mathbb{Z}$-order in $\mathcal{A}$, then

$$d(\Lambda/\mathbb{Z}) = \mathcal{N}_{K/\mathbb{Q}}(d(\Lambda/\mathcal{O}_K))d(\mathcal{O}_K/\mathbb{Z})^{n^2},$$

where $d(\mathcal{O}_K/\mathbb{Z})$ is just the usual number field discriminant of the extension $K/\mathbb{Q}$.

To summarize, we have just shown that the normalized determinant

$$\delta(\psi(\Lambda)) = 1/(m(\mathcal{C}))^{1/n}$$

is given by

$$\delta(\psi(\Lambda)) = \left(\frac{1}{|\mathcal{N}_{K/\mathbb{Q}}(d(\Lambda/\mathcal{O}_K))d(\mathcal{O}_K/\mathbb{Z})^{n^2}|}\right)^{1/2n}.$$

This reveals that we only have to consider the term

$$\mathcal{N}_{K/\mathbb{Q}}(d(\Lambda/\mathcal{O}_K))$$

as $d(\mathcal{O}_K/\mathbb{Z})^{n^2}$ is fixed (when K is fixed). The $\mathcal{O}_K$-discriminant $d(\Lambda/\mathcal{O}_K)$ is an ideal in $\mathcal{O}_K$, but $\mathcal{N}_{K/\mathbb{Q}}(d(\Lambda/\mathcal{O}_K))$ can be seen as an element in $\mathbb{Z}$. Therefore we can discuss the size of ideals of $\mathcal{O}_K$. By this, we mean that ideals are ordered by the absolute values of their norms to $\mathbb{Q}$. For example, if $\mathcal{O}_K = \mathbb{Z}[i]$, we say that the prime ideal generated by $2+i$ is smaller than the prime ideal generated by 3, because they have norms 5 and 9, respectively.

We are now ready to state the bounds that characterize the best order codes in terms of normalized minimum determinant. The hypotheses take into account that the order code can be embedded into $M_k(\mathbf{H})$, for some k.

In the following, we use the notation $2 \mid\mid n$ which means that 2 divides n, but 4 does not.

Proposition 6.5: Let $\mathcal{A}$ be a K-central division algebra of index n, $2 \mid n$, where K is a totally real number field, and let $P_1 \leq P_2$ be a pair of smallest primes in K. Let us suppose that all the infinite primes are ramified in $\mathcal{A}$.

If $2 \mid\mid n$ and $2 \mid [K:\mathbb{Q}]$, then the minimum discriminant of $\mathcal{A}$ is

$$(P_1P_2)^{k(k-1)}.$$

If $4 \mid n$ then the minimum discriminant of $\mathcal{A}$ is

$$(P_1P_2)^{n(n-1)}.$$

If $2 \mid\mid n$ and $2 \nmid [K:\mathbb{Q}]$, then the minimal discriminant of $\mathcal{A}$ is

$$P_1^{n(n-1)}P_2^{k(k-1)}.$$

Proof: The proof with related background as well as more general bounds can be found in Appendix. ■

Example 6.1: Consider the question of building a 16-dimensional lattice code in $M_4(\mathbb{C})$ with the best achievable normalized minimum determinant. The order code $\psi(\Lambda)$ gives an mn^2-dimensional lattice code in $M_{nm}(\mathbb{C})$ for any order Λ. To have $nm = 4$ and $mn^2 = 16$, the only option is to choose $m = 1$ and $n = 4$. According to Proposition 12.3, we have that the smallest possible discriminant for a $\mathbb{Q}$-central division algebra of index 4 is $2^{12} \cdot 3^{12}$. Let us now suppose that

$$\mathcal{A} = (E/\mathbb{Q}, \sigma, \gamma)$$

is the algebra having a maximal order Λ with the promised discriminant. According to Proposition 6.3 we have that

$$m(\psi(\Lambda)) = 6^6 \text{ and } \delta(\psi(\Lambda)) = \left(\frac{1}{6^{12}}\right)^{\frac{1}{8}} = 0.068...$$

Proposition 6.5 tells us that we can achieve this bound even with a 16-dimensional lattice in $M_4(\mathbb{C}) \cap M_2(\mathbf{H})$.

In [10], the authors managed to build a 16-dimensional lattice code IA-MAX in $M_4(\mathbb{C})$ having a normalized minimum determinant equal to $0.1361....$ We however conjecture that $0.068....$ is the best possible minimum determinant for a lattice in $M_4(\mathbb{C}) \cap M_2(\mathbf{H})$.

VII. Explicit construction methods

So far our study has been mostly theoretical. No explicit constructions resulting from the mapping ψ (18) have yet been given. We have only proved that the afore described matrix lattices with NVD exist. Let us now suppose that we have a K-central division algebra $\mathcal{D} = (E/K, \sigma, \gamma)$, where $[K : \mathbb{Q}] = m$ and $[E : K] = n$. There exist m $\mathbb{Q}$-embeddings β_i from K to $\mathbb{C}$. For each β_i we can find such an embedding $\sigma_i : E \hookrightarrow \mathbb{C}$ that $\sigma_i|_K = \beta_i$. Let us now suppose that $\{\sigma_1, \dots, \sigma_m\}$ is a set of representatives of embeddings β_i.

By using the left maximal representation we get an embedding $\phi : \mathcal{D} \hookrightarrow M_n(E) \subseteq M_n(\mathbb{C})$. Let us suppose that a is an element of $\mathcal{D}$ and A is the corresponding matrix $\phi(a)$. We then get a mapping

$$\psi^* : \mathcal{D} \to M_{n \times nm}(\mathbb{C}) \tag{22}$$

which is defined by

$$a \mapsto \mathrm{diag}(\sigma_1(A), \dots, \sigma_m(A)).$$

We now have the following explicit version of the previously defined embedding (18).

Proposition 7.1: Let us suppose that Λ is a $\mathbb{Z}$-order in $\mathcal{D}$ and that ψ^* is the embedding (22) defined above. Then $\psi^*(\Lambda)$ is a mn^2 dimensional lattice in $M_{mn \times nm}(\mathbb{C})$. For any non-zero element of the order Λ we have

$$det_m(\psi^*(a)) \geq 1.$$

However, in general we might loose the connection between the volume of the fundamental parallelotope of the order code $\psi^*(\Lambda)$ and the $\mathbb{Z}$-discriminant of Λ. However if we can choose the left regular representation and the embeddings $\sigma, \dots, \sigma_m$ correctly we have the following. Let us suppose that we have such a center K and an index n division algebra $\mathcal{A}$ that

$$\mathcal{A} \otimes_{\mathbb{Q}} \mathbb{R} \cong M_{n/2}(\mathbf{H})^{\omega} \times M_n(\mathbb{R})^{r_1 - \omega} \times G(\mathbb{C})^{r_2}.$$

Proposition 7.2: Let us suppose that Λ is a $\mathbb{Z}$-order in $\mathcal{A}$ and that ψ^* is the previously defined embedding. If we can choose $\sigma_1, \dots, \sigma_m$ and a left maximal representation ϕ so that

$$\psi^*(\Lambda) \subset \mathrm{diag}(M_{n/2}(\mathbf{H})^{\omega} \times M_n(\mathbb{R})^{r_1-\omega} \times G(\mathbb{C})^{r_2}),$$

we get

$$m(\psi^*(\Lambda)) = \sqrt{|d(\Lambda/\mathbb{Z})|}$$

and

$$\delta(\psi^*(\Lambda)) = \left(\frac{1}{|d(\Lambda/\mathbb{Z})|}\right)^{1/2n}.$$

Proof: Under the assumption that the embeddings and the maximal representation are chosen as presented the proof of these claims is verbatim the same as for Proposition 6.3 and can therefore found from [26]. ■

Unfortunately in the proof of the following proposition we have to use some notions not defined in this paper.

Proposition 7.3: Let us suppose we have an index n $\mathbb{Q}$-central division algebra and let ϕ denote the left regular representation. If we have such a real matrix M that

$$M\phi(\mathcal{D})M^{-1} \subseteq M_{n/2}(\mathbf{H}),$$

then

$$\delta(M\phi(\Lambda)M^{-1}) = \left(\frac{1}{|d(\Lambda/\mathbb{Z})|}\right)^{1/2n}.$$

Proof: We will give the proof in the case where the index is 2. The generalization is obvious and we will meet all the needed ideas already in this simplest case.

Let us suppose that $\phi(\Lambda)$ has a $\mathbb{Z}$-basis $\{A_1, A_2, A_3, A_4\}$. We denote $B_i = MA_iM^{-1}$ and set $\mathcal{B} = \{(B_1, \dots, B_4\}$. We can flatten the matrix B_i into a 4-tuple $L(B_i)$ by first forming a vector of length 4 out of the entries of A_i (e.g. row by row). The following identities are now easily seen

$$L(B_i)L(B_j)^T = \mathrm{Tr}(B_iB_j^T) \tag{23}$$

and

$$L(B_i)L(B_j^T)^T = \mathrm{Tr}(B_iB_j). \tag{24}$$

The Gram matrix of the lattice $M\phi(\Lambda)M^{-1}$ is

$$G = (\Re(\mathrm{Tr}(B_iB_j^{\dagger})))_{i,j=1}^4.$$

Both B_i and $B_j^{\dagger}$ do have Alamouti structure and therefore so does also $B_iB_j^{\dagger}$. This reveals that $\mathrm{Tr}(B_iB_j^{\dagger}) \in \mathbb{R}$ and we can omit taking the real part from the Gram matrix.

According to Equation (23) we can now write

$$G = (L(B_i)L(B_j^*)^T)_{i,j=1}^4 = L(\mathcal{B})L(\mathcal{B})^{\dagger},$$

where the rows of the 4×4 matrix $L(\mathcal{B})$ consist of the vectors $L(B_i)$. A simple permutation of the columns and elementary properties of determinants give us that

$$|\mathrm{det}(L(\mathcal{B}))\mathrm{det}(L(\mathcal{B})^{\dagger})| =$$

$$|\mathrm{det}(L(\mathcal{B}))\mathrm{det}(L(\mathcal{B})^T)| = |\mathrm{det}(L(\mathcal{B}))\mathrm{det}(L(\mathcal{B}')^T)|,$$

where $L(\mathcal{B}')$ is a matrix with the rows $L((B_i)^T)$. According to Equation (24) we now have

$$L(\mathcal{B})L(\mathcal{B}')^T = (\mathrm{Tr}(MA_iA_jM^{-1}))_{i,j=1}^4.$$

A general result on matrix traces tells us that $\mathrm{Tr}(XCX^{-1}) = \mathrm{Tr}(C)$ for any matrices C and X. This result combined with the definition of the discriminant now gives us that

$$L(\mathcal{B})L(\mathcal{B}')^T = (\mathrm{Tr}(MA_iA_jM^{-1}))_{i,j=1}^4 =$$

$$(\mathrm{Tr}(A_iA_j))_{i,j=1}^4 = \sqrt{d(\Lambda/\mathbb{Z})}.$$

■

Example 7.1: Consider from (15) the division algebra

$$\mathcal{D}_{Alam} = (\mathbb{Q}(i)/\mathbb{Q}, \sigma, -1),$$

which has index 2 and center $\mathbb{Q}$. The field $\mathbb{Q}$ has only one infinite place ∞ and according to Proposition 5.2 it is ramified in the algebra $\mathcal{D}_{Alam}$. We thus have an embedding $\mathcal{D}_{Alam} \hookrightarrow \mathbf{H}$ given by (19). If we choose a $\mathbb{Z}$-order Λ in $\mathcal{D}_{Alam}$, $\psi(\Lambda) \subset \mathbf{H} \subset M_2(\mathbb{C})$ is a 4-dimensional lattice code.

Here the left regular representation directly gives us an explicit version (see (22) and Proposition 7.1) of this mapping. As demonstrated in the beginning of the paper, it also gives us a fast-decodable code.

Example 7.2: Let us consider the example we gave in the very beginning of the paper. The cyclic algebra

$$\mathcal{D}_{ort} = (\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}(\sqrt{2}), \sigma, -1),$$

is an index 2 division algebra with center $\mathbb{Q}(\sqrt{2})$. Here σ is simply the complex conjugation. The general theory tells us that $\mathcal{D}_{ort}$ can be embedded into $M_2(\mathbf{H})$.

Again the mapping from Proposition 22 will directly give us an explicit version of the embedding in (19). The field $\mathbb{Q}(\sqrt{2})$ has two $\mathbb{Q}$-embeddings β_1, β_2, where $\beta_1(\sqrt{2}) = \sqrt{2}$ and $\beta_2(\sqrt{2}) = -\sqrt{2}$. The corresponding $\mathbb{Q}$-embeddings σ_1 and σ_2 are defined by the equations $\sigma_1 = id$, $\sigma_2(i) = i$ and $\sigma_2(\sqrt{2}) = -\sqrt{2}$ (or equivalently $\sigma_2(\zeta_8) = -\zeta_8$). The natural order Λ consists of elements $x = a_1 + a_2\zeta_8 + ua_3 + u\zeta_8 a_4$, where $a_i \in \mathbb{Z}[i]$. The left regular representation now gives us

$$\alpha(x) = \begin{pmatrix} a_1 + a_2\zeta_8 & -a_3^* - a_4^*\zeta_8^* \\ a_3 + a_4\zeta_8 & a_1^* + a_2^*\zeta_8^* \end{pmatrix}.$$

It is then an easy task to see that

$$\sigma_2(\alpha(x)) = \begin{pmatrix} a_1 - a_2\zeta_8 & -a_3^* + a_4^*\zeta_8^* \\ a_3 - a_4\zeta_8 & a_1^* - a_2^*\zeta_8^* \end{pmatrix}.$$

In particular both $\alpha(x)$ and $\sigma_2(\alpha(x))$ are elements in $\mathbf{H}$ and Proposition 7.2 can be applied. These results reveal that the example code we gave in the beginning of the paper was just an instance of the general theory developed above.

Remark 7.1: These two examples may give us a little too rosy picture of the power of our theory. In both cases, the embedding in Proposition 7.1 exactly imitated the embedding (19). On top of that this representation also led to codes with reduced decoding complexity. However, we do not have any guarantee that either of these things will happen more generally. It heavily depends on the chosen maximal subfield, non-norm element and even on the chosen generator of the Galois group. In Sections VIII and X we will meet situations where the left regular representation does not directly give us the required embedding even when the division algebra has the correct algebraic structure. Yet, in all these cases a simple manipulation applied after the left regular representation will give us an embedding to the matrix ring of quaternions and codes that have reduced decoding complexity. While this may seem to be accidental, there are some underlying algebraic principles that explain the sudden "luck" we encounter, see Section XI.

VIII. Fast-decodable 4×2 MIDO codes

So far, we have developed an algebraic theory of fast-decodable codes through different characterizations and bounds. We are now finally putting our theory into use to give a few different coding strategies that lead to fast-decodable codes. We start with MIDO codes for 4 Tx antennas, with the following properties:

- They are 16-dimensional lattices in $M_4(\mathbb{C})$.
- They satisfy the NVD property.
- Their decoding complexity ranges from $|S|^{10}$ to $|S|^{16}$ when a real alphabet of size $|S|$ is used.

A. A family of fast-decodable MIDO codes with $\mathbb{Q}$ as a center

We give here an example of a MIDO code built following step by step the theory developed so far. The starting point is to consider a division algebra that can be embedded into $M_2(\mathbf{H})$ via the embedding ψ (18). According to Section V and Proposition 5.2, we consider a $\mathbb{Q}$-central division algebra $\mathcal{A} = (E/\mathbb{Q}, \sigma, \gamma)$ of index 4, where E is a CM field and γ a negative non-norm element, namely

c1) $[E : \mathbb{Q}] = 4$,
c2) $\gamma, \gamma^2 \notin \mathcal{N}_{E/\mathbb{Q}}(E^*)$,
c3) $\mathrm{Gal}(E/Q) = \langle\sigma\rangle$ with $\sigma^2(f) = f^*$, where f^* stands for the complex conjugate of f, and
c4) $\gamma < 0$.

One instance of such an algebra is

$$\mathcal{D}_{mido} = (\mathbb{Q}(\zeta_5)/\mathbb{Q}, \sigma, -8/9),$$

where σ is given by $\sigma(\zeta_5) = \zeta_5^3$. The prime 2 is totally inert in the extension $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ and therefore [16, Lemma 11.1] $\mathcal{D}_{mido}$ is a division algebra.

Let $\mathcal{O}_E = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2 \oplus \mathbb{Z}w_3 \oplus \mathbb{Z}w_4$ be the ring of algebraic integers of E. The left representation ϕ^* of $\mathcal{D}_{mido}$ now yields

$$\begin{pmatrix} y_1 & \gamma\sigma(y_4) & \gamma y_3^* & \gamma\sigma(y_2)^* \\ y_2 & \sigma(y_1) & \gamma y_4^* & \gamma\sigma(y_3)^* \\ y_3 & \sigma(y_2) & y_1^* & \gamma\sigma(y_4)^* \\ y_4 & \sigma(y_3) & y_2^* & \sigma(y_1)^* \end{pmatrix}, \tag{25}$$

where $y_i = y_i(g_{4i-3}, g_{4i-2}, g_{4i-3}, g_{4i}) = g_{4i-3}w_1 + g_{4i-2}w_2 + g_{4i-3}w_3 + g_{4i}w_4$ and $g_{4i-j} \in \mathbb{Q}$ for $i = 1,2,3,4,\ j = 0,1,2,3$. If we pick up an order Λ from $\mathcal{D}_{mido}$, then $\psi^*(\Lambda)$ is a 16-dimensional lattice code with the NVD property from Proposition 7.2.

We can prove that the discriminant of this algebra meets the bound of Proposition 6.5, but even if we choose a maximal order from this algebra there is no guarantee (because we have not fulfilled the conditions of Proposition 7.2 yet) that this small discriminant would result into good normalized minimum determinant.

This is because we now face here, for the first time, the problem that the embedding ψ^* from Section VII does not directly give us an embedding into $M_2(\mathbf{H})$, although Proposition 7.1 promises that such an embedding exists. Luckily, we can perform a series of simple manipulations starting from the left regular representation that will transform the code matrices into a correct form and at the same time will recover the connection between the discriminant of the algebra and the normalized minimum determinant of the lattice.

After swapping

1) y_2 and y_3,
2) the 2nd and the 3rd column, and
3) the 2nd and the 3rd row,

we get the matrix

$$\begin{pmatrix} y_1 & \gamma y_2^* & \gamma\sigma(y_4) & \gamma\sigma(y_3)^* \\ y_2 & y_1^* & \sigma(y_3) & \gamma\sigma(y_4)^* \\ y_3 & \gamma y_4^* & \sigma(y_1) & \gamma\sigma(y_2)^* \\ y_4 & y_3^* & \sigma(y_2) & \sigma(y_1)^* \end{pmatrix}. \tag{26}$$

Next we perform the following energy balancing transformation by distributing the effect of $|\gamma|$ more evenly. By denoting $r = |\gamma|^{1/4}$, we finally get a code consisting of matrices of the desired type:

$$\begin{aligned} & X_{FD}(y_1, y_2, y_3, y_4) \qquad (27) \\ = & \begin{pmatrix} y_1 & -r^2 y_1^* & -r^3\sigma(y_4) & -r\sigma(y_3)^* \\ r^2 y_2 & y_1^* & r\sigma(y_3) & -r^3\sigma(y_4)^* \\ r y_3 & -r^3 y_3^* & \sigma(y_1) & -r^2\sigma(y_2)^* \\ r^3 y_3 & r y_2^* & r^2\sigma(y_1) & \sigma(y_1)^* \end{pmatrix}. \end{aligned}$$

The minimum determinant of the code stays unchanged since the above transformation is actually just a conjugation by a real matrix M. Let us now suppose that we have a maximal order Λ of the algebra $\mathcal{D}_{mido}$ (such an order can be found by using the computer algebra system Magma [29]). Now the new code obtained from this maximal order is $M\psi^*(\Lambda)M^{-1}$, and a direct calculation reveals that this code lattice meets the normalized minimum determinant bound $\delta(\phi(\Lambda)) = 0.068...$ (cf. Propositions 7.2, 7.3, 6.5, and Example 6.1).

To make the code suitable for PAM modulation, we further describe a modified version of this code that will have an almost rectangular shaping. The ring of algebraic integers in $\mathbb{Q}(\zeta_5)$ also has a $\mathbb{Z}$-basis $\{1-\zeta, \zeta-\zeta^2, \zeta^2-\zeta^3, \zeta^3-\zeta^4\}$, where we have abbreviated $\zeta_5 = \zeta$. The elements in the code matrix (27) now become, after further restricting the coefficients g_i to $\mathbb{Z}$:

$$\begin{aligned} y'_i &= y'_i(g_{4i-3}, g_{4i-3}, g_{4i-2}, g_{4i}) \\ &= g_{4i-3}(1-\zeta) + g_{4i-2}(\zeta-\zeta^2) + \\ &\quad + g_{4i-1}(\zeta^2-\zeta^3) + g_{4i}(\zeta^3-\zeta^4) \end{aligned}$$

and

$$\begin{aligned} \sigma(y'_i) &= g_{4i-3}(1-\zeta^3) + g_{4i-2}(\zeta^3-\zeta) \\ &\quad + g_{4i-1}(\zeta-\zeta^4) + g_{4i}(\zeta^4-\zeta^2). \end{aligned}$$

We get a set of matrices $X_{FD,A_4}(y'_1, y'_2, y'_3, y'_4)$ forming a 16-dimensional lattice code in $M_2(\mathbf{H})$. We note that the choice of $\gamma = -8/9$ prevents this order code from being a natural order. However, after multiplication by 9^4, the resulting lattice code will be included in a natural order, thus inheriting the NVD property. The geometric structure of the code is relatively close to a Cartesian product of four A_4-lattices (see [30]), therefore we call it the A_4 code. This code was also proposed for the DVB Consortium's *Call for Technologies for DVB-NGH* [31].

The variables g_{4i-j} in each of the y'_i range over a certain PAM set, so that the code encodes overall 16 independent PAM symbols. In other words, a PAM vector $(g_1, \ldots, g_{16})$ is mapped into a (4×4) matrix

$$\sum_{i=1}^{16} g_i B_i,$$

where the basis matrices B_i of the code are

$$\begin{aligned} B_1 &= X_{FD,A_4}(y'_1(1,0,0,0), 0, 0, 0), \\ B_2 &= X_{FD,A_4}(y'_1(0,1,0,0), 0, 0, 0), \\ &\vdots \\ B_{16} &= X_{FD,A_4}(0, 0, 0, y'_4(0,0,0,1)). \end{aligned}$$

A direct calculation shows that

$$\Re(\mathrm{Tr}(HB_i(HB_j)^\dagger) = 0$$

for $1 \leq i \leq 4$ and $5 \leq j \leq 8$, where H is a (2×4) channel matrix. This is exactly the design criterion of Subsection III-A described by the steps 1-2, yielding a complexity of $|S|^{12}$ for the code A_4.

We can perform yet another change of basis that will enable us to take advantage of the steps 3-4 described in Subsection III-A. The new basis

$$\left\{1, \frac{\zeta+\zeta^{-1}}{2}, \frac{\zeta-\zeta^{-1}}{2}, \frac{\zeta^2-\zeta^{-2}}{4}\right\}$$

will result in a complexity $|S|^{10}$, reduced by as much as 37.5% from the full complexity $|S|^{16}$ of a general MIDO code. However, it is not an integral basis, hence the minimum determinant is small though still non-vanishing.

The resulting lattice has almost cubic shaping, but, due to the coding gain loss, the performance is approximately 1 dB worse than that of the A_4 version. The promised complexity reduction is due to the fact that the first two basis elements are real, while the last two are purely imaginary. Hence the relations given by the steps 1-4 in III-A are all satisfied.

Remark 8.1: To the best of our knowledge, there is no guarantee that an integral basis consisting of $n/2$ real and $n/2$ purely imaginary elements even exists.

Remark 8.2: The matrix manipulations given in this section may also seem to have a somewhat *ad hoc* feeling. Yet we will see in Sections X and XI that this strategy can be used far more generally to give us embeddings to $M_k(\mathbf{H})$.

Remark 8.3: We also simulated the maximal order code from this algebra achieving the discriminant bound and the A_4 code under spherical shaping. Both codes had equally good performance, gaining almost 1 dB compared to the linearly dispersed A_4. It seems that the A_4 code did inherit the good performance of the optimal maximal order code.

B. MIDO codes from a bigger center through puncturing

We now adopt a slightly different approach to the design problem of MIDO codes via puncturing of MIMO codes. We start from the matrix (14)

$$\begin{pmatrix} x_0 & i\sigma(x_3) & i\sigma^2(x_2) & i\sigma^3(x_1) \\ x_1 & \sigma(x_0) & i\sigma^2(x_3) & i\sigma^3(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & i\sigma^3(x_3) \\ x_3 & \sigma(x_2) & \sigma^2(x_1) & \sigma^3(x_0) \end{pmatrix}$$

and puncture it in two different ways.

Let us first repeat a remark made above, namely that $\mathbb{Q}(\zeta_5+\zeta_5^{-1}) = \mathbb{Q}(\sqrt{5})$ is a subfield of $\mathbb{Q}(\zeta_5)$. As a first puncturing, we restrict ourselves to elements in $\mathbb{Q}(\sqrt{5})$ instead of $\mathbb{Q}(\zeta_5)$. Note that since $\sigma^2(\zeta_5) = \zeta_5^4$, we further have

$$\sigma^2(\zeta_5+\zeta_5^{-1}) = \zeta_5^4+\zeta_5^{-4} = \zeta_5^{-1}+\zeta_5$$

and thus $\mathbb{Q}(\sqrt{5})$ is fixed by σ^2. This yields a codebook $\mathcal{C}_1$ consisting of codewords of the form

$$X = \frac{1}{\sqrt{5}}\begin{pmatrix} x_0 & i\sigma(x_3) & ix_2 & i\sigma(x_1) \\ x_1 & \sigma(x_0) & ix_3 & i\sigma(x_2) \\ x_2 & \sigma(x_1) & x_0 & i\sigma(x_3) \\ x_3 & \sigma(x_2) & x_1 & \sigma(x_0) \end{pmatrix}. \tag{28}$$

It is now enough to notice that we are working in the same field extension as for the Golden code [25], meaning that we can use the same shaping technique. Denote:

$$\begin{aligned} \theta &= \frac{1+\sqrt{5}}{2}, \\ \sigma(\theta) &= \frac{1-\sqrt{5}}{2} = 1-\theta, \\ \alpha &= 1+i-i\theta, \\ \sigma(\alpha) &= 1+i-i\sigma(\theta). \end{aligned}$$

Every entry x_j in the above matrix is now taking the form

$$x_j = \alpha(a_j+b_j\theta),\ j=0,1,2,3,$$

where $a_j, b_j \in \mathbb{Z}[i]$ are chosen to be QAM symbols. We thus indeed get a MIDO code carrying 8 complex QAM symbols, with unitary encoding matrix yielding the cubic shaping property. The factor $\frac{1}{\sqrt{5}}$ is used to normalize the minimum determinant to one.

A straightforward calculation gives that the volume of the fundamental parallelotope of this code is $5^4 \cdot 2^8$. At the same time, the minimum determinant of the code is 1. If we now scale the code $\mathcal{C}_3$ with $(\frac{1}{5^4 \cdot 2^8})^{1/16}$, the resulting code lattice $\mathcal{C}_3^* = (\frac{1}{5^4 \cdot 2^8})^{1/16} \cdot \mathcal{C}_3$ has a fundamental parallelotope of volume 1. We now see that the normalized minimum determinant of the lattice $\mathcal{C}_3^*$ is

$$\left[\left(\frac{1}{5^4 \cdot 2^8}\right)^{1/16}\right]^4 = \frac{1}{20}.$$

Comparing this to Proposition 6.2, we conclude that the normalized minimum determinant of the code $\mathcal{C}_3$ is very close to the optimum minimum determinant of orthogonally shaped MIDO codes. The good performance of this code once again suggests that it is favorable for the code performance at low SNRs to maintain the cubic shaping.

Take again a codeword

$$\begin{pmatrix} x_0 & i\sigma(x_3) & ix_2 & i\sigma(x_1) \\ x_1 & \sigma(x_0) & ix_3 & i\sigma(x_2) \\ x_2 & \sigma(x_1) & x_0 & i\sigma(x_3) \\ x_3 & \sigma(x_2) & x_1 & \sigma(x_0) \end{pmatrix}$$

and multiply both the 3rd and 4th column by ζ_8^{-1}, where $\zeta_8 = e^{2i\pi/8}$ is a primitive 8th root of unity. Then multiply the 3rd and 4th row this time by ζ_8. Note that this of course brings the matrix entries out of the algebra we started with, but will do this without changing the determinant. We further note that we can use $\gamma = -i$ instead of $\gamma = i$, since $-i$ is not a norm. The proof of this fact is similar to that of the non-norm element i (cf. IV-A), and follows from the same argument of the transitivity of the norm. We have to show that there cannot be an element with norm $-i$ over $\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(i)$. If there were an element a with $\mathcal{N}_{\mathbb{Q}(\sqrt{5},i)/\mathbb{Q}(i)}(a) = -i$, then ia would have norm

$$i^2 \mathcal{N}_{\mathbb{Q}(\sqrt{5},i)/\mathbb{Q}(i)}(a) = i,$$

a contradiction. Again for the case of $\mathcal{N}_{\mathbb{Q}(\sqrt{5},i)/\mathbb{Q}(i)}(a) = \gamma^2 = -1$ we refer the reader to [16, Section 8].

We now obtain for the codebook $\mathcal{C}_3$ consisting of matrices

$$\begin{pmatrix} x_0 & -i\sigma(x_3) & -\zeta_8 x_2 & -\zeta_8\sigma(x_1) \\ x_1 & \sigma(x_0) & -\zeta_8 x_3 & -\zeta_8\sigma(x_2) \\ \zeta_8 x_2 & \zeta_8\sigma(x_1) & x_0 & -i\sigma(x_3) \\ \zeta_8 x_3 & \zeta_8\sigma(x_2) & x_1 & \sigma(x_0) \end{pmatrix}. \qquad (29)$$

Let us denote by $\mathbf{c}_1$, $\mathbf{c}_2$, $\mathbf{c}_3$ and $\mathbf{c}_4$ the 4 columns of the above matrix. It can be easily seen that the above manipulations result in having columns 1 and 3, and 2 and 4 satisfying

$$\mathbf{c}_1^T \mathbf{c}_3 = 0, \ \mathbf{c}_2^T \mathbf{c}_4 = 0$$

without changing the shaping. This construction thus increases the "orthogonality-likeness" of the columns of the code without altering its other properties. Though this transformation does increase the number of zeroes in the R-matrix of the QR decomposition, it does not reduce the decoding complexity as defined. This is due to the fact that, albeit the above relations resemble the real inner product, the vectors $\mathbf{c}_i$ actually consist of complex elements.

We now propose another puncturing, which focuses this time on having orthonormal columns, in order to have provable fast decodability. Since $\mathbb{Q}(\zeta_5, i) = \mathbb{Q}(\zeta_{20})$, where $\zeta = \zeta_{20} = e^{2i\pi/20}$ is a primitive 20th root of unity, we can alternatively take as basis for $\mathbb{Q}(i, \zeta_5)$ the set $\{1, \zeta, \zeta^2, \zeta^3\}$. An element x is then written as

$$x = a + b\zeta + c\zeta^2 + d\zeta^3, \ a, b, c, d \in \mathbb{Q}(i).$$

We perform the following puncturing and restriction of coefficients. Take x_0, x_1 of the form

$$a + ib\zeta + c\zeta^2 + id\zeta^3, \ a, b, c, d \in \mathbb{Z}$$

so that $\sigma^2(x_0) = x_0{}^*$, $\sigma^2(x_1) = x_1{}^*$. For x_2 and x_3, take instead

$$a(1+i) + b(1-i)\zeta + c(1+i)\zeta^2 + d(1-i)\zeta^3, \ a, b, c, d \in \mathbb{Z}$$

to get this time $\sigma^2(x_2) = -x_2{}^*$, $\sigma^2(x_3) = -x_3{}^*$. This results in a codebook $\mathcal{C}_2$ with codewords given by

$$X = \begin{pmatrix} x_0 & i\sigma(x_3) & -x_2{}^* & i\sigma(x_1)^* \\ x_1 & \sigma(x_0) & -x_3{}^* & -\sigma(x_2)^* \\ x_2 & \sigma(x_1) & x_0{}^* & -\sigma(x_3)^* \\ x_3 & \sigma(x_2) & x_1{}^* & \sigma(x_0)^* \end{pmatrix}. \qquad (30)$$

An easy computation shows that the 1st and 3rd row, resp. the 2nd and 4th row, are orthonormal. By permuting the 2nd and 3rd rows and columns resp., we get

$$X_{\mathcal{C}_2}(x_0, x_1, x_2, x_3) = \begin{pmatrix} x_0 & -x_2^* & i\sigma(x_3) & i\sigma(x_1)^* \\ x_2 & x_0^* & \sigma(x_1) & -\sigma(x_3)^* \\ x_1 & -x_3^* & \sigma(x_0) & -\sigma(x_2)^* \\ x_3 & x_1^* & \sigma(x_2) & \sigma(x_0)^* \end{pmatrix} \qquad (31)$$

which clearly exhibits the Alamouti block structure of the code.

As previously for the A_4-code, a PAM vector $(g_1, \dots, g_{16})$ is mapped into a (4×4) matrix

$$\sum_{i=1}^{16} g_i B_i,$$

where the basis matrices B_i are

$$\begin{aligned} B_1 &= X_{\mathcal{C}_2}(x_0(1,0,0,0), 0, 0, 0), \\ B_2 &= X_{\mathcal{C}_2}(x_0(0,1,0,0), 0, 0, 0), \\ &\vdots \\ B_{16} &= X_{\mathcal{C}_2}(0, 0, 0, x_3(0,0,0,1)). \end{aligned}$$

Again a direct calculation gives

$$\Re(\mathrm{Tr}(HB_i(HB_j)^\dagger) = 0$$

for $1 \le i \le 4$ and $5 \le j \le 8$ and a complexity of $|S|^{12}$.

C. The Srinath-Rajan (SR) code

So far, the best performing fast-decodable 4×2 code has been the code based on stacked CIODs proposed in [5]. The real and imaginary parts of the encoded symbols are separated in a careful way, so that when a rotated 4- or 16-QAM alphabet is used, the code has high coding gain. It is moreover conjectured that the code has the NVD property, but this has not been proved. Before rotating the constellation, the code is equivalent to transmitting four independent Alamouti blocks A, B, C, D:

$$X_{\text{SR unrotated}} = \begin{pmatrix} A & \zeta_8 B \\ \zeta_8 C & D \end{pmatrix},$$

where a primitive 8th root of unity ζ_8 has been added in order to maximize the coding gain of the rotated code. Because the blocks are independent prior to rotation, the unrotated code does not have full diversity. For this reason, getting a proof for the possible NVD by using the theory developed in this paper does not seem possible.

If we ignore the constant ζ_8, the code is exactly of the same form as the codes proposed in this paper (except possibly for the NVD), as clearly

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in M_2(\mathbf{H}).$$

Adding the constant ζ_8 does not affect fast decodability, but helps to maximize the coding gain.

We have not tried whether it is possible to improve the coding gain of the codes proposed in this paper by using a suitable rotation. This may be seen as a reason for the small performance loss of the proposed codes compared to the rotated SR code. We did however try another type of optimization, namely using a spherical constellation instead of linearly dispersed constellation (cf. VI-A). The spherically shaped fast-decodable code outperforms the SR code (see Section IX below) by a fraction of a dB.

IX. Simulation results of MIDO codes

In Figure 1, we have plotted the block error rates of different MIDO codes at the rate 4 bpcu. All of the codes use the 2-PAM or 4-QAM alphabet, except for the spherically shaped A_4 code referred to as $NC\,(FD, A4, \text{spher.})$. This code is constructed by using a 6-PAM alphabet and then choosing the codewords with the smallest Frobenius norms, resulting in a codebook with 2^{16} codewords.

We can see that the punctured code $\mathcal{C}_2$ ($NC\,(FD, \text{punct.})$) does not perform too well due to its small (though non-vanishing) coding gain. The other new codes, for their part, perform more or less equally to the Biglieri-Hong-Viterbo (BHV) code. The A_4 code ($NC\,(FD, A4)$) is slightly beaten by the BHV code at low-moderate SNRs, but will eventually outperform it starting from 20 dB, thanks to its full diversity. The shaped code ($NC\,(\text{shaped})$), which is not fast-decodable, outperforms the BHV code starting from 16 dB. The Srinath-Rajan (SR) code with a rotated 4-QAM constellation wins the BHV code by a fraction of a dB. The spherically shaped A_4 outperforms the BHV and SR codes by roughly 0.5 dB, and performs slightly better compared to the best previously known MIDO code IA-MAX [10]. The code IA-MAX is constructed from a certain maximal order, and has higher decoding complexity. It is added here for the sake of completeness in comparison.

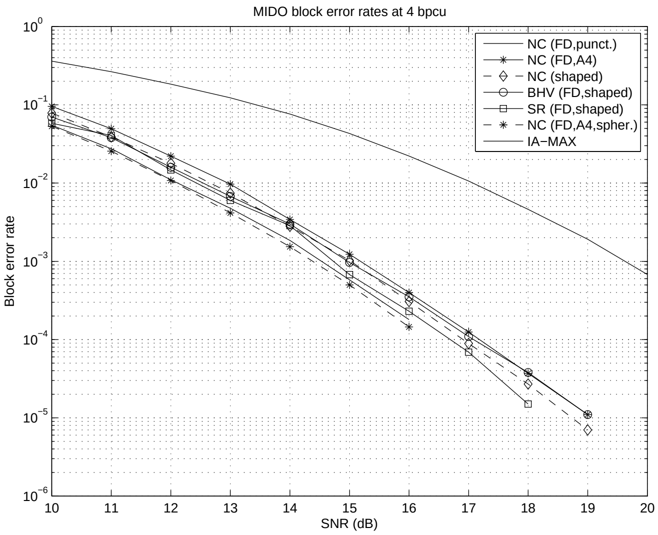

Fig. 1. Comparison among different MIDO codes at rate 4 bpcu.

Let us point out that we have not optimized any of the proposed codes by *e.g.* rotating the constellation. Just out of interest, we simulated the unrotated SR code, and the performance got somewhat worse than that of the A_4 code. Hence, we also expect some improvement in the performance of our codes, when an optimal rotation is used.

We can also use the maximal order of the A_4 code algebra, which will result in similar performance as the IA-MAX and spherically shaped A_4 code. While the maximal order codes are not fast-decodable, the spherically shaped A_4 code still uses the same linear dispersion matrices and hence admits fast decodability. However, an extra step is required to check that the decoded word really belongs to the codebook. For a detailed description of the required changes in a sphere decoder, see [32]. As a conclusion, sticking to linear dispersion and natural orders causes a penalty of about 0.5 dB in the BLER performance. On the other hand, it seems that the requirement of fast-decodability itself does not cause any performance loss. This is hardly a surprise, as the proposed constructions are nothing but orders of cyclic division algebras, which have been shown to have excellent performance [16], [33], [10].

X. Fast-decodable codes for the 6×3 and 6×2 channels

Let us now extend our code constructions to six transmit antennas. While this paper mainly deals with MIDO codes, *i.e.*, codes for two receivers, here we also consider the case of three receivers. The reason for this is that the embedding (18)

$$\psi : \mathcal{A} \hookrightarrow \text{diag}(M_{n/2}(\mathbf{H})^m)$$

into to a matrix ring of the Hamiltonian quaternions naturally yields codes with dimension rate $R_1 = n$, which is also the number of Tx antennas. Thus, for six transmitters we have $R_1 = 6$, which is ideal for reception with three antennas. From this, we can construct a code suitable for two receivers ($R_1 = 4$) by puncturing. The so-called *smart puncturing* [34], [10] will be applied in order to further reduce the decoding complexity, while maintaining a low peak-to-mean power ratio (PAPR).

A. Construction for the 6×3 channel

We build our (6×6) code matrix analogously to the (4×4) case (cf. Subsection VIII-A). To this end, we consider the index-six cyclic algebra

$$\mathcal{A} = (\mathbb{Q}(\zeta_7)/\mathbb{Q}, \sigma : \zeta_7 \mapsto \zeta_7^3, -3/4)$$

built upon the 7th cyclotomic field. Since -3 is inert ($(3 \bmod 7)$ generates the whole group $\mathbb{Z}_7^*$), the element $\gamma = -3/4$ is a non-norm element and $\mathcal{A}$ is a division algebra. As the center $\mathbb{Q}$ is totally real and only has one infinite place which is ramified, we have an embededding $\mathcal{A} \hookrightarrow M_3(\mathbf{H})$.

Let us now build the embedded code matrix more explicitly. We start by noting that

$$\sigma^3(x) = x^*$$

for all $x \in \mathbb{Q}(\zeta_7)$, and hence, taking into account that $\sigma(x^*) = \sigma(x)^*$, we get

$$\sigma^4(x) = \sigma(x)^*, \quad \sigma^5(x) = \sigma^2(x)^*.$$

We can again start with the left regular representation and perform some simple manipulation on the resulting matrix: first, we swap the 2nd and the 4th row, and the 3rd and the 5th row. After this, we swap the 3rd and the 4th row. Next, we do the same for the columns. Let us denote this intermediate form by X'. Then we balance the effect of γ to get a more unified energy distribution among the antennas. This can be done by conjugating the matrix X' by the matrix

$$P = \text{diag}(r, r^2, r, r^2, r, r^2),$$

where $r = \sqrt{|\gamma|}$. Finally, we do the exchange $x_3 \leftrightarrow x_1$ and $x_4 \leftrightarrow x_2$, followed by $x_2 \leftrightarrow x_3$. The final form of the code matrix now becomes

$$X = PX'P^{-1} = \begin{pmatrix} A & B & C \end{pmatrix}, \tag{32}$$

where each

$$A = \begin{pmatrix} x_0 & -rx_1^* \\ rx_1 & x_0^* \\ x_2 & -rx_3^* \\ rx_3 & x_2^* \\ x_4 & -rx_5^* \\ rx_5 & x_4^* \end{pmatrix}, \tag{33}$$

$$B = \begin{pmatrix} -r^2\sigma(x_5) & -r\sigma(x_4)^* \\ r\sigma(x_4) & -r^2\sigma(x_5)^* \\ \sigma(x_0) & -r\sigma(x_1)^* \\ r\sigma(x_1) & \sigma(x_0)^* \\ \sigma(x_2) & -r\sigma(x_3)^* \\ r\sigma(x_3) & \sigma(x_2)^* \end{pmatrix}, \tag{34}$$

and

$$C = \begin{pmatrix} -r^2\sigma^2(x_3) & -r\sigma^2(x_2)^* \\ r\sigma^2(x_2) & -r^2\sigma^2(x_3)^* \\ -r^2\sigma^2(x_4) & -r\sigma^2(x_5)^* \\ r\sigma^2(x_5) & -r^2\sigma^2(x_4)^* \\ \sigma^2(x_0) & -r\sigma^2(x_1)^* \\ r\sigma^2(x_1) & \sigma^2(x_0)^* \end{pmatrix} \tag{35}$$

consist of three Alamouti blocks.

The encoding can be performed similarly as in the 4×2 case. Let us denote the 36 basis matrices by

$$\begin{aligned} B_1 &= B_1(x_0(1,0,0,0,0,0),0,0,0,0,0), \\ &\vdots \\ B_2 &= B_2(x_0(0,1,0,0,0,0),0,0,0,0,0), \\ B_{36} &= B_{36}(0,0,0,0,0,x_5(0,0,0,0,0,1)). \end{aligned}$$

We then form a finite code by setting

$$\mathcal{C}_{6\times 3} = \{\sum_{i=1}^{36} g_i B_i \mid g_i \in \mathcal{G}\},$$

where $\mathcal{G} \subseteq \mathbb{Z}$ is, for instance, a Q-PAM alphabet.

B. Decoding

Let us now consider the sphere decoding process as described in III for the code (32). Following the above notation, we notice that the code lattice has six basis matrices $B_1, \ldots, B_6$ of the form

$$\begin{pmatrix} x_0 & & & & & \\ & x_0^* & & & & \\ & & \sigma(x_0) & & & \\ & & & \sigma(x_0)^* & & \\ & & & & \sigma^2(x_0) & \\ & & & & & \sigma^2(x_0)^* \end{pmatrix},$$

and six basis matrices $B_7, \dots, B_{12}$ of the form

$$\begin{pmatrix} A' & 0 & 0 \\ 0 & B' & 0 \\ 0 & 0 & C' \end{pmatrix},$$

where

$$A' = \begin{pmatrix} 0 & -rx_1^* \\ rx_1 & 0 \end{pmatrix},$$

$$B' = \begin{pmatrix} 0 & -r\sigma(x_1)^* \\ r\sigma(x_1) & 0 \end{pmatrix},$$

and

$$C' = \begin{pmatrix} 0 & -r\sigma^2(x_1)^* \\ r\sigma^2(x_1) & 0 \end{pmatrix}.$$

A straightforward calculation shows that

$$\Re(\text{Tr}(HB_i(HB_j)^\dagger)) = 0$$

for $1 \leq i \leq 6,\ 7 \leq j \leq 12$ and any channel matrix H. Hence, the (36×36) R-matrix of the QR decomposition has a (6×6) zero block in the corresponding position, and the (12×12) upper left corner of R looks like

$$\begin{pmatrix} R^{1,1} & 0 \\ 0 & R^{2,2} \end{pmatrix},$$

where the blocks $R^{i,i}$ are (6×6) matrices. From this we see that the symbols $g_1, \dots, g_6$ can be decoded independently of the symbols $g_7, \dots, g_{12}$, resulting in complexity $2|S|^{30}$ instead of the full complexity $|S|^{36}$. Further reductions are possible by a change of basis, similarly as in the 4×2 case. By forming the basis of elements half of which are real and the other half purely imaginary (cf. VIII-A), we get more zeros in the R matrix. In that case we again have, for any channel matrix H, that

$$\Re(\text{Tr}(HB_i(HB_j)^\dagger)) = 0$$

for $1 \leq i \leq 6,\ 7 \leq j \leq 12$, but further also get

$$\Re(\text{Tr}(HB_i(HB_j)^\dagger)) = 0$$

for $1 \leq i \leq 3,\ 4 \leq j \leq 6$ and $7 \leq i \leq 9,\ 10 \leq j \leq 12$, resulting in complexity $4|S|^{27}$.

C. *Construction for the 6×2 channel by puncturing*

In order to construct a 6×2 MIDO code, we will next consider a punctured version of the above code. The puncturing affects the shape of the code lattice, so different puncturing will give a different lattice and whence also different performance. One obvious option is to keep an eye on the Gram matrix of the lattice – the closer it is to a (scaled) identity matrix, the better the shape. A smart puncturing may also aid the decoding process, namely we may puncture the basis matrices that cause nonorthogonality. On the other hand, it is not a good idea to puncture all six basis matrices corresponding to one of the elements x_i in (32), because this will cause zeros in the encoding matrix and hence increase the PAPR.

Here we provide just one possible puncturing, to give the reader an idea as to how one may go about it. Let us denote the basis matrices as in the previous section by $B_1, \dots, B_{36}$. We puncture the following basis matrices

$$\begin{aligned} \text{in } x_2 : &\quad B_{13}, B_{14}, B_{15}, \\ \text{in } x_3 : &\quad B_{19}, B_{20}, B_{21}, \\ \text{in } x_4 : &\quad B_{25}, B_{26}, B_{27}, \\ \text{in } x_5 : &\quad B_{31}, B_{32}, B_{33}. \end{aligned}$$

The resulting code will still have the same orthogonality relations as the original code, but will only have 24 basis elements giving us decoding complexity $4|S|^{15}$.

XI. Further generalizations via conjugations of the left-regular representation

As already pointed out, we can always embed a division algebra into a matrix ring of the Hamiltonian quaternions, provided that the center is totally real and all of its infinite places ramify. For all such division algebras, we have that $\sigma^{n_t/2}(x) = x^*$, $\sigma^{j+n_t/2}(x) = \sigma^j(x)^*$, and $\gamma < 0$. The embedding

$$\psi : \mathcal{A} \hookrightarrow \text{diag}(M_{n/2}(\mathbf{H})^m),$$

however, will only give us the existence of a fast-decodable code with dimension rate $n = n_t$.

In what follows, we are going to show how to overcome the problem of the implicit nature of the map ψ. Once we have constructed a CDA $\mathcal{A} = (E/\mathbb{Q}, \sigma, \gamma)$ of the required form, the explicit map $\psi : \mathcal{A} \to M_{n_t/2}(\mathbf{H})$ is given as follows.

Proposition 11.1: Let X denote the left regular representation matrix of an element $a = x_0 + ux_1 + \cdots + u^{n_t-1}x_{n_t-1} \in \mathcal{A}$. Then

$$\psi(X) = BPX(BP)^{-1} \in M_{n_t/2}(\mathbf{H}),$$

where the elements $P(i,j)$, $1 \leq i, j \leq n_t$, of the permutation matrix P are

$$P(i,j) = \begin{cases} 1, & \text{if } \ 2 \not| \, i \ \text{ and } \ j = \frac{i+1}{2}, \\ 1, & \text{if } \ 2 \,|\, i \ \text{ and } \ j = \frac{i+n_t}{2}, \\ 0, & \text{otherwise} \end{cases}$$

and

$$B = \text{diag}(\sqrt{|\gamma|}, |\gamma|, \dots, \sqrt{|\gamma|}, |\gamma|)$$

is the energy balance matrix.

Proof: Let us first consider the columns of X, and denote $X = (1, \sigma, \ldots, \sigma^{n_t-1})$ to represent the fact that the first column is mapped by the identity element, the second is mapped by σ, etc. In order to get the required Alamouti block form, we need to reorder the columns as

$$(1, \sigma^{n_t/2}, \sigma^2, \sigma^{2+n_t/2}, \ldots, \sigma^{n_t/2-1}\sigma^{n_t-1}),$$

so that σ^j is followed by its conjugate for all j. This is done exactly by post-multiplying X by P^{-1}.

Next we have to rearrange the rows. Notice first that, by ignoring γ, the rows of XP^{-1} look like

$$\left(\begin{array}{cccc} a_1 & b_1^* & \ldots & a_{n_t/2} & b_{n_t/2}^* \\ c_1 & d_1^* & \ldots & c_{n_t/2} & d_{n_t/2}^* \\ \vdots & \vdots & & \vdots & \vdots \\ s_1 & t_1^* & \ldots & s_{n_t/2} & t_{n_t/2}^* \\ \hline b_1 & a_1^* & \ldots & b_{n_t/2} & a_{n_t/2}^* \\ d_1 & c_1^* & \ldots & d_{n_t/2} & c_{n_t/2}^* \\ \vdots & \vdots & & \vdots & \vdots \\ t_1 & s_1^* & \ldots & t_{n_t/2} & s_{n_t/2}^* \end{array}\right)$$

where the horizontal line divides the matrix in two parts each having $n_t/2$ rows. We easily see that the Alamouti block form can be achieved by pairing the rows as

$$(1, n_t/2+1), (2, n_t/2+2), \ldots, (n_t/2, n_t).$$

This is done by pre-multiplying XP^{-1} by P, *i.e.*, we conjugate X by P. As the last step, we should take care of the effect of γ. By conjugating PXP^{-1} further by $B = \mathrm{diag}(\sqrt{|\gamma|}, |\gamma|, \ldots, \sqrt{|\gamma|}, |\gamma|)$, the elements γ will appear in each (2×2) block of the matrix as follows:

$$\begin{pmatrix} (\pm)\sqrt{|\gamma|} & (\pm)|\gamma| \\ (\pm)|\gamma| & (\pm)\sqrt{|\gamma|} \end{pmatrix}.$$

In addition, the plus and minus signs are automatically rearranged by this conjugation so that the resulting matrix consists of Alamouti blocks. ■

Remark 11.1: After Proposition 11.1, we can algebraically optimize the normalized minimum determinant. Namely, the resulting parallelotope will be exactly that given by Proposition 7.3. Notice that this was not the case before the conjugation, for while the conjugation does not affect the non-normalized minimum determinant, it does affect the measure of the fundamental parallelotope and hence the normalized minimum determinant!

Now that we have an explicit form of the mapping ψ, the fast-decodability property can be seen as follows: with $\mathbb{Q}$ as the center ($m=1$), the R-matrix of the QR decomposition of the matrix B (cf. III) will consist of $(n\times n)$ blocks $R^{i,j},\ 1 \le i,j \le n$, where

$$R^{1,2} = R^{3,4} = \cdots = R^{n-1,n} = \mathbf{0}_{n\times n} \tag{36}$$

and the diagonal blocks $R^{i,i},\ 1 \le i \le n$, are block-diagonal:

$$R^{i,i} = \begin{pmatrix} P^{1,1} & 0 \\ 0 & P^{2,2} \end{pmatrix}_{n\times n}. \tag{37}$$

The zero blocks (36) result from the Alamouti block structure and offer us a reduction of n real dimensions. The diagonal block structure (37) is due to the fact that when we construct the algebra upon a complex multiplication field, we can always choose a basis in which half of the elements are real and the other half purely imaginary. This, for its part, provides us with further reduction by $\frac{n}{2}$ dimensions. Hence, the decoding complexity will be of order

$$\le |S|^{n_t^2 - n_t - \frac{n_t}{2}} = |S|^{n_t^2 - \frac{3n_t}{2}},$$

where the factor ${n_t}^2$ is the exhaustive search complexity.

By puncturing, we obtain fast-decodable codes suitable for any number of receivers. The complexity of the punctured code is at most

$$|S|^{n_t R_1 - \frac{3n_t}{2}},$$

where $R_1 \le n_t$ is the dimension rate. For $n_r = 2$, we get a complexity reduction of $\frac{4n_t - 2.5n_t}{4n_t} = 37.5\%$ as promised. However, this may require a non-integral basis, and hence cause performance loss compared to an integral basis. With an integral basis, we get a reduction of $\frac{4n_t - n_t}{4n_t} = 25\%$ while guaranteeing a high coding gain.

In Table II we have summarized the complexities for $n_t = 4, 6, 8$ and $2 \le n_r \le \frac{n_t}{2}$ as an example.

TABLE II
COMPLEXITIES OF THE PROPOSED FAST-DECODABLE CODES.

$n_t \times n_r$	R_1	$n_t R_1 - \frac{3n_t}{2}$	Comp.reduction$/n_t R_1$
4×2	4	10	37.50%
6×3	6	27	25.00%
6×2	4	15	37.50%
8×4	8	52	18.75%
8×3	6	36	25.00%
8×2	4	20	37.50%
$\vdots$	$\vdots$	$\vdots$	$\vdots$

XII. CONCLUSIONS

In this paper, fast-decodable asymmetric lattice space-time codes were studied, proposing one possible generalization of the Alamouti code and the quasi-orthogonal codes to any even number of transmit antennas n_t and for any dimension rate $R_1 \leq n_t$. The codes allow linear ML processing with *e.g.* a sphere decoder for any number of receivers $\geq R_1/2$, but with lower dimensionality (less variables per linear equation). It was explicitly shown how such novel constructions follow from general algebraic principles by embedding a division algebra into a matrix ring $M_k(\mathbf{H})$ of the Hamiltonian quaternions. All this is in strong contrast to the previous *ad hoc* constructions of fast-decodable codes that have been specific to a certain number of antennas and lacking an obvious generalization. The proposed codes furthermore enjoy the NVD property, a property that no other fast-decodable MIDO code found in the literature has been proved to have.

We mainly considered the 4×2 MIDO case suitable for DVB-NGH, but also provided constructions for the 6×2 and 6×3 cases. The explicit embeddings obtained in these situations were shown to be fully generalizable to any even number of Tx antennas. Simulations were presented to show that the performance of the proposed codes is comparable to the best known MIDO codes. The achieved complexity reduction up to 37.5% is also among the best known for the MIDO channel.

In addition, a complete solution to the discriminant minimization problem for division algebras with arbitrary centers was given. As an application a normalized minimum determinant bound for code lattices in $M_k(\mathbf{H})$ was derived from the algebraic results.

Acknowledgments

The research of R. Vehkalahti and C. Hollanti is supported by the Emil Aaltonen Foundation's Young Researcher's Project, and by the Academy of Finland grant #131745.

This research was partly carried out during the visit of C. Hollanti at the Nanyang Technological University, Singapore. The research of F. Oggier is supported in part by the Singapore National Research Foundation under Research Grant NRF-RF2009-07 and NRF-CRP2-2007-03, and in part by the Nanyang Technological University under Research Grant M58110049 and M58110070.

References

[1] F. Oggier, R. Vehkalahti, and C. Hollanti, "Fast-decodable MIDO codes from crossed product algebras," in *Proc. 2010 IEEE Int. Symp. Inform. Theory (ISIT)*, Austin, TX, June 2010.

[2] F. Oggier, C. Hollanti, and R. Vehkalahti, "An algebraic MIDO-MISO code construction," in *Proc. 2010 International conference on signal processing and communications (SPCOM 2010)*, Bangalore, India, July 2010.

[3] R. Vehkalahti, C. Hollanti, and J. Lahtonen, "A family of cyclic division algebra based fast-decodable 4×2 space-time block codes," in *Proc. 2010 Int. Symp. Inf. Theory and its Appl. (ISITA)*, Taichung, Taiwan, Oct. 2010, to appear.

[4] E. Biglieri, Y. Hong, and E. Viterbo, "On fast-decodable space-time block codes," *IEEE Trans. Inform. Theory*, vol. 55, no. 2, 2009.

[5] K. P. Srinath and B. S. Rajan, "Low ML-decoding complexity, large coding gain, full-diversity STBCs for 2×2 and 4×2 MIMO systems," *IEEE J. on Special Topics in Signal Processing: Managing Complexity in Multi-user MIMO Systems*, pp. 916–927, 2010.

[6] S. M. Alamouti, "A simple transmitter diversity scheme for wireless communications," *IEEE J. Select. Areas Commun.*, pp. 1451–1458, Oct. 1998.

[7] C. Hollanti, J. Lahtonen, and H.-F. Lu, "Maximal orders in the design of dense space-time lattice codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4493 – 4510, Oct. 2008.

[8] DVB Project, the global standard for digital television. [Online]. Available: *http://www.dvb.org.*

[9] F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, "Perfect space time block codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3885–3902, Sept. 2006.

[10] C. Hollanti and H.-F. Lu, "Construction methods for asymmetric and multi-block space-time codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1086 – 1103, 2009.

[11] H.-F. Lu and C. Hollanti, "Optimal diversity multiplexing tradeoff and code constructions of constrained asymmetric MIMO systems," *IEEE Trans. on Inform. Theory*, vol. 56, no. 5, May 2010.

[12] A. Hottinen, Y. Hong, E. Viterbo, C. Mehlführer, and C. F. Mecklenbruker, "A comparison of high rate algebraic and non-orthogonal stbcs," in *Proc. 2007 ITG/IEEE Workshop on Smart Antennas WSA*, Vienna, Austria, Feb. 2007.

[13] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Inf. Theory*, vol. 45, pp. 1456–1467, Jul. 1999.

[14] G. R. Jithamithra and B. S. Rajan, "A quadratic form approach to ML decoding complexity of STBCs," preprint available at *arxiv.org/abs/1004.2844.*,.

[15] G. S. Rajan and B. S. Rajan, "Multi-group ML decodable collocated and distributed space time block codes," *IEEE Transactions on Information Theory*, vol. 56, pp. 3221–3247, July 2010, preprint available at *arxiv.org/pdf/0712.2384.*

[16] R. Vehkalahti, C. Hollanti, J. Lahtonen, and K. Ranto, "On the densest MIMO lattices from cyclic division algebras," *IEEE Trans. on Inform. Theory*, vol. 55, no. 8, pp. 3751–3780, Aug. 2009.

[17] B. Hassibi and M. Hochwald, "High-rate codes that are linear in space and time," *IEEE Trans. Inf. Theory*, vol. 48, no. 7, pp. 1804–1824, Jul. 2002.

[18] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: performance criterion and code construction," *IEEE Trans. Inf. Theory*, vol. 44, pp. 744–765, Mar. 1998.

[19] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2596–2616, Oct. 2003.

[20] J.-C. Belfiore and G. Rekaya, "Quaternionic lattices for space-time coding," in *Proc. IEEE Information Theory Workshop*, Paris, 31 March - 4 April 2003.

[21] E. Viterbo and J. Boutros, "A universal lattice code decoder for fading channel," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 1639–1642, Jul. 1999.

[22] F. E. Oggier, J.-C. Belfiore, and E. Viterbo, “Cyclic division algebras: A tool for space-time coding,” *Foundations and Trends in Communications and Information Theory*, vol. 4, no. 1, pp. 1–95, 2007.

[23] C. Hollanti, “Order-theoretic methods for space-time coding: Symmetric and asymmetric designs,” Ph.D. dissertation, Lab. of Discrete Mathematics, Turku Centre for Computer Science (TUCS), 2009, *TUCS Dissertations Series*, no. 111, *https://oa.doria.fi/handle/10024/43000*.

[24] A. A. Albert, *Structure of Algebras*. New York: American Mathematical Society, 1939.

[25] J.-C. Belfiore, G. Rekaya, and E.Viterbo, “The Golden code: a 2 × 2 full-rate space-time code with non-vanishing determinants,” in *Proc. 2004 IEEE Int. Symp. Inform. Theory*, Chicago, IL, June 27-July 2 2004, p. 308.

[26] J.-P. C. Eva Bayer-Fluckiger and J. Chaubert, “Euclidean minima and central division algebras,” *International Journal of Number Theory*, vol. 5, pp. 1155–1168, 2009.

[27] I. Reiner, *Maximal Orders*. New York: Academic Press, 1975.

[28] J. Lahtonen and R. Vehkalahti, “Dense MIMO matrix lattices - a meeting point for class field theory and invariant theory,” in *Proc. Applied Algebra, Algebraic Algorithms, and Error Correcting Codes (AAECC-17)*, Bangalore, India, 2007.

[29] MAGMA Computational Algebra System, Univ. of Sydney, Sydney, Australia. [Online]. Available: *http://magma.maths.usyd.edu.au/magma/*

[30] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, ser. Grundlehren der mathematischen Wissenshaften. Springer, 1988, vol. 290.

[31] C. Hollanti, R. Kumar, J. Lahtonen, H.-F. F. Lu, and R. Vehkalahti, “Space-time block codes for the 2Tx + 2Rx and 4tx + 2rx antenna MIMO systems,” *DVB TM-H NGH Call for Technologies (CfT) Proposal*, 2010.

[32] C. Hollanti and K. Ranto, “Maximal orders in space-time coding: Construction and decoding,” in *Proc. 2008 Int. Symp. Inf. Theory and its Appl. (ISITA)*, Auckland, New Zealand, Dec. 2008.

[33] K. R. Kumar and G. Caire, “Space-time codes from structured lattices,” *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 547 – 556, 2009.

[34] C. Hollanti and H.-F. Lu, “Constructing asymmetric space-time codes with the smart puncturing method,” in *Proc. 2006 IEEE Int. Symp. Inform. Theory*, Toronto, ON, Jul. 2008.

[35] R. Vehkalahti, “Class field theoretic methods in the design of lattice signal constellations,” Ph.D. dissertation, 2008, *TUCS Dissertations Series*, no. 100, *https://oa.doria.fi/handle/10024/36604*.

Appendix

In this Appendix we are going to present some basic results from the theory of central simple algebras and in particular from the theory of Hasse-invariants. These results are needed only in Section VI.

For a quick introduction we refer the reader to [16] and [35] where similar optimization has been done.

Let us consider a K-central division algebra of index n. Then attached to each pair $(\mathcal{A}, P)$, where P is a prime of K, is a positive rational number $h_P = a/m_P$, the so-called *Hasse-invariant* of $\mathcal{A}$ at P. The Hasse invariants of $\mathcal{A}$ fulfill the following. When P is a prime ideal of K, then

$$h_P = \frac{a}{m_P}, \quad 0 \le a < m_P \le n,\ (a, m_P) = 1,$$

when P is infinite and real, then

$$h_P = 1/2 \text{ or } h_P = 0,$$

and when P is infinite and complex, then

$$h_P = 0.$$

The number m_P is called the *local index* at prime P (see Section V-A). We say that the algebra $\mathcal{D}$ is *ramified* at the prime P, if $h_P \neq 0$. The Hasse invariants define the algebraic structure of a division algebra and in particular the discriminant of the algebra.

Proposition 12.1: Assume that $P_1, \ldots, P_s$ are a set of finite prime ideals of $\mathcal{O}_K$ and $P_{s+1}, \ldots, P_n$ are a set of real primes.

Assume further that a sequence of rational numbers

$$\frac{a_1}{m_{P_1}}, \ldots, \frac{a_s}{m_{P_s}}, \frac{a_{s+1}}{m_{P_{s+1}}}, \ldots, \frac{a_n}{m_{P_n}},$$

subject to the restriction that when $i > s$, $a_i/m_{P_i} = 1/2$, satisfies

$$\sum_{i=1}^{n} \frac{a_i}{m_{P_i}} \equiv 0 \pmod{1},$$

$1 \le a_i \le m_{P_i}$, and $(a_i, m_{P_i}) = 1$.

Then there exist a K-central division algebra $\mathcal{A}$ that has local indices m_{P_i} and the least common multiple (LCM) of the numbers $\{m_{P_i}\}$ as an index.

If Λ is a maximal $\mathcal{O}_K$-order in $\mathcal{A}$, then the discriminant of Λ is

$$d(\Lambda/\mathcal{O}_K) = \prod_{i=1}^{s} P_i^{(m_{P_i}-1)\frac{[\mathcal{A}:K]}{m_{P_i}}}.$$

We have the following two general results.

Theorem 12.2 ([16]): Let us suppose that we have a number field K and an integer n, where $4 \mid n$ or $2 \nmid n$. If $P_1 \le P_2$ is a pair of smallest primes in $\mathcal{O}_K$, then there exists a K-central division algebra of index n having a maximal order with the $\mathcal{O}_K$-discriminant

$$(P_1 P_2)^{n(n-1)}.$$

This is the smallest possible discriminant for an order inside any K-central division algebra of index n.

The following result is from [35], but is presented here for he first time in an article.

Theorem 12.3 ([35]): Let $\mathcal{A}$ be a K-central division algebra of index $2k = n$, where k and 2 are relatively prime and let $P_1 \le P_2$ be a pair of smallest primes in $\mathcal{O}_K$.

If K has at least two real primes, then there exists a K-central division algebra of index n having a maximal order with the discriminant

$$(P_1P_2)^{k(k-1)}.$$

If K has only one real prime P_∞, then there exists a K-central division algebra of index n having a maximal order with the discriminant

$$P_1^{n(n-1)}P_2^{k(k-1)}.$$

This is the smallest possible discriminant of all orders of index n division algebras with center K.

We have now given completely general discriminant bounds for any center and for any index n.

Proposition 12.4: Let $\mathcal{A}$ be a K-central division algebra of index n, $2 \mid n$, where K is a totally real number field, and let $P_1 \leq P_2$ be a pair of smallest primes in K. Let us suppose that all the infinite primes are ramified in $\mathcal{A}$.

If $2 \mid\mid n$ and $2 \mid [K:\mathbb{Q}]$, then the minimal discriminant of $\mathcal{A}$ is

$$(P_1P_2)^{k(k-1)}.$$

If $4 \mid n$ then the minimal discriminant of $\mathcal{A}$ is

$$(P_1P_2)^{n(n-1)}.$$

If $2 \mid\mid n$ and $2 \nmid [K:\mathbb{Q}]$, then the minimal discriminant of $\mathcal{A}$ is

$$P_1^{n(n-1)}P_2^{k(k-1)}.$$

Proof: In the proofs of Theorems 12.3 and 12.2 the general strategy was to choose a set of H-invariants that will yield an index n division algebra (see Theorem 12.1) and then prove that our choice was the best possible. We will use the same strategy here, but the difference is that we can do the optimization over division algebras that are totally ramified at infinite primes.

The assumption of ramified infinite primes always gives us m non-trivial Hasse invariants $\{h_{P_1}, \dots, h_{P_m}\}$, where $h_{P_i} = \frac{1}{2}$ and P_i are all the infinite primes in K.

The Hasse-invariants at infinite places do not contribute anything on discriminant of the division algebra. If we have an index n division algebra, the contribution of a Hasse-invariant $h_P = \frac{s}{m_P}$, where m_P is the local index at finite prime P, to the $\mathcal{O}_K$-discriminant is $P^{(m_P-1)\frac{n}{m_P}}$. Therefore in most cases we can simply prove the minimality of the corresponding discriminant by showing that, despite the extra ramification at infinite primes, we can choose a set of Hasse-invariants that will give us an index n division algebra with a discriminant reaching the bound 12.3 or 12.2.

In Table III we have collected the Hasse-invariants (at finite places) of the algebras we claim to be optimal.

TABLE III

index	[K:Q]	H-invariants at finite places
odd		-
4k	odd	$h_{P_1} = \frac{1}{4k}$, $h_{P_2} = \frac{2k-1}{4k}$
4k	even	$h_{P_1} = \frac{1}{4k}$, $h_{P_2} = \frac{k-1}{4k}$
2k, $2 \nmid k$	even	$h_{P_1} = \frac{1}{k}$, $h_{P_2} = \frac{k-1}{k}$
2k, $2 \nmid k$	odd	$h_{P_1} = \frac{k-2}{2k}$, $h_{P_2} = \frac{1}{k}$

In addition to what is said in the table about the H-invariants at the finite places, we suppose that each of these algebras have H-invariants $\frac{1}{2}$ at all the infinite primes. By a direct calculation we can see that in each case we get a division algebra of index n with all the infinite primes ramified. This will take care of the first two claims of the proposition. In the first case, where $2 \mid\mid n$ and $2 \mid [K:\mathbb{Q}]$, the division algebra given in the table will reach the claimed bound which coincides with the general bound in 12.3. In the case $4 \mid n$ the algebras given in Table III reach the bound 12.3 and we are done with the second claim.

We are left with the case, where $2 \mid\mid n$ and $2 \nmid [K:\mathbb{Q}] = m$. In this case the problem is that while the sum of the $m-1$ first infinite Hasse-invariants is an integer, there is still one extra infinite H-invariant $h_{P_m} = \frac{1}{2}$ we have to take care of. Therefore we are forced to choose Hasse-invariants $h_{P_1} = \frac{k-2}{2k}$ and $h_{P_2} = \frac{1}{k}$ for the finite places. The proof that this set of Hasse-invariants will give us the optimal discriminant is verbatim the same as it is for the case where the center has exactly one real place. This case was dealt in the proof of Proposition 12.3 and we refer the reader to [35].

■